Ethical Hacking: Rationale for a hacking methodological approach to network security

Regina D. Hartley

East Carolina University

Abstract

The purpose of this study is to address the issues and concerns of network security professionals due to the prominence of information technologies and growing dependence on the Internet. Growing concern stems from the apparent lack of security inherent within information technologies and information systems. Such topics as identity theft and the latest computer virus are addressed in light of inherent dangers and implications from attackers world wide. Particular emphasis is placed upon the need for determining a potential proactive measure to improve network security. Measures consisting of a hacking methodology in network security to combat the exacerbating topics associated with the Internet and computer networks world wide are examined. The study includes a history of hacking, investigation into present day issues and concerns, and topics such as cyber terrorism, identity theft, and economical considerations are focused on. The study concludes by examining ethical hacking as a viable solution to network security concerns. Distinctive concentration will examine successful programs within the public and private sectors concerning penetration testing and ethical hacking.

Ethical Hacking: Rationale for a hacking methodological approach to network security

The prominence of information technologies and growing dependence on computers continues to infiltrate all of society. Growing concern stems from the apparent lack of security inherent within information technologies and information systems. Of particular importance is our growing reliance on the Internet and networking capabilities. The Internet has provided vast opportunities in a wide array of areas that were impossible in prior years. Today we are able to access colossal amounts of information, visit untold locations world wide, and communicate in unprecedented ways.

Along with the positive facets of the Internet and networking capabilities unpleasant aspects also exist. While various crimes have existed for many years, the Internet and information technology have brought it into our homes and businesses in unimaginable ways. Criminals of today have a new platform for conducting activities, and many individuals are so bewildered at the subsequent onslaught from these endeavors that in many cases only reactive measures may be implemented. From identity theft to the latest computer virus, few appear immune from the inherent dangers and implications from attackers world wide.

The purpose of this paper is to suggest and defend a potential proactive measure to improve network security. Measures consisting of a hacking methodology in network security to combat the exacerbating issues associated with the Internet and computer networks world wide. The discussion begins with a history of hacking with the premise that through this examination and appropriate definitions a better understanding may be gleaned into the mystery surrounding the topic of hacking.

The next area of study will investigate present day issues and concerns with particular emphasis on the intensity of attacks in recent months. Additional topics covered will address critical aspects such as cyber terrorism, identity theft, and economical considerations. The third area will scrutinize ethical hacking highlighting the positive aspects of hackers culminating in a proper definition of ethical hacking as a viable approach to network security. Finally, the study will address educational aspects of network security. Distinctive concentration will feature successful programs within the public and private sectors concerning penetration testing and ethical hacking.

History of Hacking

The Beginning

To better understand the need for proactive measures relating to information security, attention is focused upon the history of hacking. Hacking began for the most part in the 1960s and originated on the campuses of Massachusetts Institute of Technology (MIT) and Stanford University. At that time the word “hack” actually referred to programming shortcuts, and was considered a cleaver way to complete tasks faster. These original hackers or, “old school hackers,” were not interested in hacking for malicious reasons, but rather simply enjoyed technology (Slatalla, 2005).

The second generation of hackers during the 1970s, known as the “Elder Days,” targeted the telephone system. The Internet had not as of yet become prominent as a means of communication nor a primary target to explore. During this time “Phone Phreaks” emerged, and one such phreak was John Draper known to the underground world as “Cap'n Crunch.” Draper made the discovery that a toy whistle inside Cap'n Crunch cereal had the same 2600 megahertz signal as the phone system and could be

used to access AT&T's long-distance switching system. Draper designed and built “blue boxes” that could be used with this whistle to allow other “phreaks” to make free long distance phone calls. Interestingly enough, Steve Wozniak and Steve Jobs, the future founders of Apple Computer, begin by making and selling blue boxes (Slatalla, 2005).

The third era of hacking is referred to as the “Golden Age,” and covers the time period between 1980 through 1991. During this time hacker message boards emerge as do various hacking groups such as the Legion of Doom and the Chaos Computer Club. Also during this time a popular movie, "War Games," introduces the public to the term “hacking.” Perhaps inspired by the movie, six teenagers are arrested for breaking into the phone system. They are referred to as the “414 gang” which is the area code they are traced back to (Slatalla, 2005).

This brings us to the “Great Hacker War.” The Legion of Doom and Masters of Deception begin an online war lasting almost two years by jamming telephone lines. This is the first of many online wars that will continue to plague innocent individuals. During this time there is a shift in emphasis from the telephone to the Internet. Also during this time hacker publications, “’Zines” begin such as the “2600” publication and “Phrack” (Slatalla, 2005).

Between 1986 and 1994 the US government passes legislation due to the prominence of people, businesses, and hackers entering the Internet. In 1986, Congress passes the Computer Fraud and Abuse Act making it a crime to break into computer systems. Two years later, the world experiences the first self-replicating worm released by Robert T. Morris, Jr. Morris, a Cornell University Graduate student, is the first convicted under the new law (Slatalla, 2005).

Other events to make news in the hacker community feature the two Kevins, Kevin Poulsen and Kevin Mitnik. Kevin Pousen and friends crack a phone used in a radio station call-in contest. This enables only their phone calls to get through, and they are able to "win" two Porsches, $20,000 in cash, and vacation trips until being caught. Kevin Mitnik was able to break into systems that were seemingly impossible to penetrate; he is caught and sentenced to a year in prison. Mitnick is caught again in 1995, and is accused of stealing 20,000 credit card numbers. This becomes a very sore topic for the hacking community due to the very negative light in which Mitnick is portrayed and the subsequent movie produced entitled "Take Down" (Slatalla, 2005).

This time period ranged from 1994 to 1998 and is considered a shift in which hackers lost their romantic appeal to the public. The Internet was becoming more commercialized and ecommerce was beginning to thrive. To make matters worse, a gang led by Russian hacker, Vladimir Levin, is charged with breaking into Citibank's computers and siphoning $10 million. As the year 2000 approached, the Y2K hysteria loomed and zero tolerance became a very serious matter (Slatalla, 2005).

The Year 2000 and Beyond

After the Y2K panic is past, the Internet, now becoming more prominent, develops into somewhat of a playground for many so called "hackers". In defense, old school hackers coin the term "crackers" to separate themselves from those seeking to perform destructive acts via the Internet. New categories of crackers and attackers emerge (Slatalla, 2005).

One new category of cracker to emerge is "script kiddies," who are composed of individuals generally between the ages of 12-30. Most are male, Caucasian, and appear

very bright and as such become bored in school. Many get caught for getting into systems due to bragging online, and their intent is to vandalize or disrupt systems (Slatalla, 2005).

A second category of attacker or cracker is professional criminals. Most of these individuals have been generally performing crimes all along, but now use the Internet due to ease of perpetration and execution. They make a living by breaking into systems and selling the information (Slatalla, 2005).

The final group, coders and virus writers, consider themselves a select group due to their extensive programming expertise. They typically write code for a virus or malicious software then make it available on their private networks called "zoos," and leave it to others to release it into "The Wild" or Internet. Their inflection of damage and apparent lack skill makes them very unpopular with the hacking community (Slatalla, 2005).

Following the review of hacking history, the analysis will concentrate on the present concerns and development of the Internet. Attention will highlight common methods of attack, terrorist activity, and conclude with recent statistics.

Present Concerns and Evolution of the Internet

Common Methods of Attacks

In recent years, viruses have begun to plague anyone wishing to utilize the Internet much to the exasperation of security professionals which further necessitates the need for proactive measures from security professionals. Viruses start out as simply nuisances, then quickly move to macro viruses causing code to execute on a computer when an email attachment is opened. When the public becomes savvy to the malicious

code, their writers provide attractive names tantalizing victims to open the email to see inside (Ethical Hacking: student courseware).

Many of these viruses, which are actually worms that self propagate, also contain programming code that enables attackers to acquire information from the victim's computer. Most current viruses contain password stealing Trojans, send emails further replicating itself over the Internet, and can send a victim's system information, usernames, passwords, and similar information back to the worm's author. Many also disable the computer's antivirus program, create a backdoor, or entrance for the attacker, and may also install a "keylogger" which is a program that records all the keystrokes on the computer (Ethical Hacking: Student courseware).

In recent months, however, Internet users have been inundated with viruses that do not wait to be opened; mere connection to the Internet is all that is needed. Recent viruses target machines making them zombies for denial of service purposes or for the lucrative task of sending spam. Perpetrators of the viruses are able to gain access to computers connected to the Internet through the use of a Trojan program that hides the virus within a legitimate looking program. After acquiring a computer, now known as a zombie, the attacker can use this computer to distribute a denial of service attack to any server on the Internet. A denial of service attack results when many computers request information. This causes the server to be overloaded, and typically results in the inability to respond to legitimate user access which may cost the business lost revenue.

In addition to uses of zombies to cause denial of service attacks, virus writers sell zombies to spammers who use the unsuspecting victim's computer to send spam or junk email (Joris, 2005). Many spamming campaigns are works of compromised systems.

Spammers are sold IP addresses by virus writers and coders who have virtual networks of zombie computers known as “botnets” (Roberts, 2005).

To exacerbate the present concern over connection to the Internet, “Phishing” and “Pharming” have become common practice by attackers for unlawful profit despite unfailing efforts by security professionals. “Phishing” attacks are email fraud and arrive in a victim’s email as a legitimate request for information. Unsuspecting recipients of the emails are lured to an attacker’s web site under the guise of updating pertinent account information. In addition, some victims are redirected to web sites that install spyware or Trojan programs allowing backdoor on their computers whereby attackers may enter at will (Shor, 2005).

As concerns over “Phishing” attacks have become public, attackers have altered their methodology to include “Pharming.” This method of deceit “poisons" a DNS server and redirects individuals on the Internet to an attacker’s web server. To the computer user, the web site looks legitimate even in the browser window, but once again the victim is conned into providing pertinent personal data (Vamosi, 2005,).

While common methods of attack are quite serious, the next section will address a more crucial matter of terrorism. The Internet has assisted terrorists in their attacks in unprecedented ways.

Terrorist Organizations

Not only are attacks from individuals interested in securing access onto computer systems for illicit gain a security concern, but attacks from terrorist organizations also pose significant trepidation on the part of security professionals. An interview conducted with a hacker who assists the US Government, who was not identified, provided insight

into the severity of the problem. He states "there are two different forms of mapping going on right now. One form of mapping is automated systems ....we refer to as zombies.… The other form of mapping is much more sophisticated … they are looking for critical systems…. So somebody is essentially preparing for a large-scale attack, or perhaps more subtle attacks on American critical infrastructure" (Frontline: Cyber war).

Another concerned individual with the National Infrastructure Protection Center is Michael Vatis. He goes on to share his concern with the "big spike" in number of cases involving organized criminal groups for illicit financial gain. Vatis also states his concern about cyber terrorism and shutting down of critical systems. This last fact is based upon terrorist groups and their use of information technology in a "very robust way" (Frontline: Cyber war).

David Verton has written a book entitled "Black Ice: The Invisible Threat of Cyber-Terrorism. This book is based upon his research into this growing area of concern. In November 2000, a simulation was conducted entitled "Black Ice." Verton indicates that as a result of this simulation evidence was found that a "growing number of critical interdependencies … and how devastating combined cyber-attacks and physical attacks can be." He goes on to add that a "Significant amount of evidence … indicates terrorism may be evolving toward a more high tech future at a faster rate than previously believed," and that Al-Qaeda has "more interest in cyber-terrorism than previously believed" (Verton, 2003).

In the next segment, recent studies have provided statistical data indicating some alarming trends. These studies further substantiate a need for heightened security measures on the part of security professionals.

Year 2005 Statistics

Recent statistics are quite disturbing and further expound evidence that security measures implemented by today's security professionals require a more proactive approach. The 2005 Computer Crime and Security Survey provided by the Computer Security Institute and the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad addressed a host of security concerns. According to data received from the 2004 survey, virus attacks continue to be the greatest source of financial losses. Unauthorized access was the second highest contributing factor of financial losses, and denial of service attacks was third. Alarmingly, unauthorized use of computer systems has increased, and web site incidents have increased significantly (Gordon, Loeb, Lucyshyn, Richardson, 2005).

Another disconcerting set of statistics is provided by Symantec Corporation, a leading provider in security. According to a recent Internet Security Threat Report, "phishing" continues to increase, and during the first six months of 2005 Symantec blocked a total of 1.04 billion "phishing" attacks. This amount, compared to 546 million in the last six moths of 2004, indicates an increase of 90% in this type of attack. Moreover, the first half of 2005 documented almost 11,000 new viruses and worms which is an increase of 48% from the previous six months. This is an astounding increase of 142% from the first half of 2004 indicating this is fast becoming the most popular method of assault (Online Fraud: An Update).

The next section in the study will focus on ethical hacking as a methodology of proactively addressing security concerns of professionals. The presupposition associated with ethical hacking is merely that of a different approach to security. Ethical hacking is

primarily penetration testing and is argued by many professions to be potentially more robust and accurate when measuring the security of a network.

Ethical Hacking

A close scrutiny of the area of ethical hacking will highlight some positive aspects of hacking. This study could propitiously offer a rationale and a better understanding for constructing proactive measures necessary to develop a viable approach to network security.

Hackers

A hacker may be defined as a ”person who enjoys learning the details of computer systems and how to stretch their capabilities….One who programs enthusiastically or who enjoys programming rather than just theorizing about programming” (Ethical Hacking: Student courseware).

According to a Frontline documentary on Hackers, one may perceive hackers in a new light. One such individual interviewed, Robert Steele, suggested that “It’s very erroneous to think of hackers as criminals—that’s not the case….Hackers have been identifying major vulnerabilities in Microsoft products and … all kinds of computer and communication products. And nobody has wanted to listen.” Mr. Steele goes on to recommend that hackers are a power unto themselves, as a “community of vibrant knowledge.” He adds that hackers have been portrayed in a negative light by the media. Steele suggests that the real culprit is software vendors due to the lack of standards or licenses required to write software. He further adds that our “Entire digital society is based on software by people we don’t know, have no licenses, quality control, or legal liability” (Frontline: Hackers: interviews: Robert Steele).

Reid and Count Zero, two hackers who formed “Cult of the Dead Cow” which is a hacking group most notable for creating a hacking tool called Back Orafice, also impart expanded substantiation supporting hackers. Count Zero states “Microsoft has the world's most popular operating systems installed on 90 percent of the computers in the world …. Unfortunately those people are wide open to attack of various kinds.” He goes on to add “I'm very concerned that we make sure we get it right in terms of the security.…And if we don't get it right, it's just going to be a big mess, and that scares me a little” (Frontline: Hackers: interviews: Reid and Count Zero).

Countless individuals share in their concerns regarding Microsoft. They feel that Microsoft has sent products to the market long before perfecting and removing any security flaws or issues. One such individual is Paul Strassmann who feels strong enough about this issue to go on record suggesting that Microsoft is a threat to US security (Frontline: Hackers: Who’s responsible).

As a matter of fact many hackers have attempted to utilize their hacking expertise to the betterment of network security. One such hacker was caught breaking into NASA’s computers and states “I would email the system administrators sometimes and tell them that their computers were vulnerable. I would tell them … how to fix the problems….Three weeks later … I still had access to their computers…” (Frontline: Hackers: Anonymous).

The next segment in the examination of ethical hacking will address the fundamental ethical perspectives particularly as it relates to information technology. This analysis will begin with appropriate definitions of what constitutes ethics.

Ethical Perspectives

Many theories and perspectives of ethics abound providing insight into underlying ethical foundations of an individual's behavior. "Equipped with the knowledge that information technologies have become a necessity, one may safely conclude that ethical issues involving computers will continue to be a topic of discussion among organizational leaders" (DeLisse, 2000). Ethics is particularly important with regard to computer use due to the nature of technology and ethical dilemmas attributable to information. "When faced with alternative courses of action or alternative goals to pursue, ethics helps us to make the correct decision" (Laudon, 1995, p. 34).

Some researchers state that ethical behavior is relative. Negative and positive declarations of ethical relativism suggest the lack of universal moral rights and wrongs; morality becomes relative to one's society (Johnson, 1994). The basic philosophy is "everyone ought to act so as to bring about the greatest amount of happiness for the greatest number of people" (Johnson, 1994, p. 24).

Other researchers categorize ethical actions by emphasizing the internal nature of the act itself. What makes an action right or wrong is the principle inherent in the action (Johnson, 1994). Many ethicists feel that motivation to act ethical or unethical within in given situation lies within the individual, while others believe it is comprised primarily from outside forces (Laudon, 1995).

The prior two sections have addressed hackers and ethics, and now the analysis will proceed on to ethical hacking. In the following segment, hacking may be viewed within an ethical perspective.

Ethical Hacking

Following the review of hackers, the discussion now attends to the topic of ethical

hacking. This methodology for assisting professionals in their endeavors to secure networks will be examined in light of its effectiveness for proactive measures.

Ethical hacking may be defined as the “methodology adopted by ethical hackers to discover the vulnerabilities existing in information systems’ operating environments.” There are a number of classes of hackers such as Black Hats who are highly skilled, but have malicious and destructive intent. White Hats, in contrast, are hackers who use their expertise for defensive security analyses, and Gray Hats who hack for different reasons either ethically or unethically depending on the situation (Ethical Hacking: Student courseware).

One of the more effective ways of testing network security in recent months is penetration testing or ethical hacking which is similar in concept to hiring external auditors. Organizations are increasingly using this methodology to evaluate the effectiveness of information security. These activities are used to identify and exploit security vulnerabilities thereby providing the organization with the necessary information to implement corrective measures (Using an Ethical Hacking Technique).

According to one researcher, "security of the Internet is broken and 'ethical hacking' has evolved as part of the potential solution." He goes on to suggest that "'ethical hacking' may be one of the most effective ways to proactively plug rampant security holes"(Yurcik, Doss, 2001). An increasing number of security experts are advising “organizations to hire ethical hackers--aka white hat hackers--as consultants to carry out penetration testing of their networks" (Leung, 2005).

The finally portion of the study will examine the educational aspects of equipping professionals within the field of network security. Concentration will highlight

successful programs within the public and private sectors concerning penetration testing and ethical hacking.

Ethical Hacking Education

A wide range of educational opportunities exist for individuals interested in pursuing information security. Many of these are being offered in the public sector within community colleges and universities. It is interesting to note that while many schools offer such education and training, a number of professionals express concern about teaching hacking techniques. This apprehension stems from a fear that students may use the information unethically. Educational institutions prevail over this assumption by offering concepts within an ethical framework (Sanders, 2003).

Community Colleges and Universities

Northern Virginia Community College received a $250,000 grant in 2002 for implementing a network security certificate. Their course offerings emphasize an ethical focal point to encourage the concept of "ethical hackers." George Mason University in Fairfax, VA offers courses in information warfare and also encapsulates all concepts within an "ethical framework" (Thurrott, 2005).

Syracuse University offers a Cyber Security Boot Camp to prepare future technology security leaders. Topics include cybersecurity, cryptography, steganography, digital forensics, network security, and wireless security. There are rigorous requirements for entry, and the Boot Camp ends with "Hackfest" which provides a more hands on approach to theoretical concepts covered (Carnevale, 2005).

In Paris, a school called Zi Hackademy boasts of a wide variety of students from all over France. The teacher, Clad Strife, is a local high school student who demonstrates

his hacking expertise. The school's philosophy is "only if you become a hacker can you understand how hackers think and operate" (van der Laan, 2001).

A researcher from Weber State University reviewed 36 schools designated as Centers of Excellence in Information Assurance Education by the United States National Security Agency. This program is provided by the National Security Agency to help prepare graduates for careers in information assurance and computer security. Upon graduation students agree to work for the federal government for a set period of time in security related positions. The researcher used the information to create a program at Weber State University (Logan, 2002).

In addition to the core requirements as designated by the United States National Security Agency, the researcher proposed a capstone course. This course would allow "hands-on" application. To counteract the concerns of administrators over teaching the "methodology of hacking" a number of precautionary measures were enlisted. An ethics component was added requiring students to sign a code of ethics, and only seniors were permitted into the capstone that had "matured in the curriculum." This combined with required pre-requisites was used to discourage anyone from attending the course just for purposes of learning the hacking methodology. Also included in the program was a criminal justice component that examined "not only the methods of entry and detection, but legal outcomes" (Logan, 2002).

Ethical Hacker Certification Boot Camps

The private sector has been very successful at offering a vast array of educational opportunities for security professional. Many firms offer “boot camps” of intense instruction lasting from 5 to 10 days and costs range from $2000 to $5000. A research

firm, IDC, projects that the number of security professionals will grow to over 800,000 by 2008, and according to many professional “more of them need to think like hackers to be effective” (McGee, 2005).

Intense School is one such provider of "ethical-hacker boot camps". When asked if any “shady characters” are taking the same training, they state that most participants are from government agencies and corporations (McGee, 2005). Other suppliers of boot campus include The Academy, NetCom Information Technology, and CertificationCity.

The leading supplier of the certification program for ethical hacking is Ec-Council. They boast of the C|EH (Ethical Hacking Certification) as being the “fastest growing certification in the security industry.” Their program contains 22 modules that cover a variety of topics, techniques, and hacking tools (Ethical Hacking: Student courseware).

With industry trends and increased instances of computer attacks, security professionals will increasingly seek out institutions providing training and education in the areas of ethical hacking and network security. Opportunities in to acquire this training and education are available through both public and private institutions.

Conclusion

The importance of information technologies and reliance on the Internet continues to permeate all aspects of our lives and society. Security issues relating to technology and information systems world wide are causing many security professionals to examine more proactive approaches to securing networks.

The purpose of this paper has been to suggest a hacking methodology approach to network security. The discussion began with a history of hacking, and continued to the

analysis of current issues and concerns with particular emphasis on the intensity of attacks in recent months.

Particular topics addressed were cyber terrorism, identity theft, and economical considerations. This was followed by an examination of ethical hacking highlighting both positive aspects of hacking and appropriate definitions of hackers, ethics and ethical hacking. The study concluded with scrutiny of the educational aspects of network security which highlighted successful programs both within the public and private sectors.

References

Carnevale, D. (2005, September 23). Basic training for anti-hackers: An intensive summer program drills students on cybersecurity skills. Chronicle of Higher Education, 52(5), pp. 41-41.

DeLisse, R. L. (2000). Rationale for computer ethics policies and a model policy for the north carolina community college system. (ERIC Document Reproduction Services No. ED 457932).

Ethical Hacking: Student courseware. Ec-Council. www.eccouncil.org;

Frontline: Hackers: Anonymous. Retrieved September 25, 2005 from http://www.pbs.org.

Frontline: Cyber war: Interviews: Hacker. Retrieved September 25, 2005 from http://www.pbs.org.

Frontline: Hackers: interviews: Michael Vatis. Retrieved September 25, 2005 from http://www.pbs.org.

Frontline: Hackers: Who's responsible?. Retrieved September 25, 2005 from http://www.pbs.org.

Frontline: Hackers: interviews: Reid and Count Zero. Retrieved September 25, 2005 from http://www.pbs.org.

Frontline: Hackers: interviews: Robert Steele. Retrieved September 25, 2005 from http://www.pbs.org.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., Richardson, R. (2005) 2005 CSI/FBI crime and security survey. Retrieved November 20, 2005 from http://www.gocsi.com.

Joris, E. (2005, July 6). *Hacking for dollars.* Retrieved November 22, 2005 from http://www.zdnet.com.

Laudon, K. C. (1995). Ethical concepts and information technology. Communications of the ACM, 38, 33-39.

Leung, L. (2005, June 20). Hackers for hire: Bringing in ethical hacker consultants is the latest in security defense. Retrieved November 5, 2005 from http://www.networkworld.com.

Logan, P. Y. (2002). Crafting an undergraduate information security emphasis within information technology. Journal of Information Systems Education, 13(3), pp. 177-182 2002

McGee, M. K. (2005, June 23). Hacker boot camp helps good guys outsmart internet troublemakers. Retrieved November 20, 2005 from http://www.informationweek.com.

Online Fraud: An Update. (2005, November 8). Retrieved November 20, 2005 from http://www.symantec.com.

Roberts, P. (2005, November 3). California man charged with botnet offenses. Retrieved November 5, 2005 from http://www.eweek.com.

Sanders, A. D. (2003). Utilizing simple hacking techniques to teach system security and hacker identification. Journal of Information Systems Education, 14(1), p. 5.

Shor, Susan. (2005, August 12). *Two Phishing Scams Target PayPal, eBay Users.* Retrieved November 23, 2005 from http://www.technewsworld.com.

Slatalla, M. A brief history of hacking. Retrieved November 5, 2005 from http://tlc.discovery.com.

Thurrott, S. Anyone can hack; it's defending the system that's cool. Retrieved November 20, 2005 from http://www.course.com.

Using an Ethical Hacking Technique to Assess Information Security Risk. (2003). The Canadian Institute of Chartered Accountants. Retrieved November 20, 2005 from http://www.cica.ca/itac.

van der Laan, N. (2001, December 3). Hackademy: Paris school offiers primer for cyberPirates. Christian Science Monitor, 94(7).

Verton, D. (2003). Black ice: The invisible threat of cyber-terrorism. McGraw Hill: Emeryville, CA.

Yurcik, B. S., Doss, D. (2001). Ethical hacking: The security justification. Ethics of Electronic Information in the 21 Century Symposium. Univeristy of Memphis: Memphis TN.

Vamosi, R. (2005, February 18). Alarm over pharming attacks: identity theft made even easier. Retrieved October 28, 2005 from http://cnet.com.