

Methods to Hacking

Methods to Hacking and Cyber Invasion

Methods to Hacking and Cyber Invasion

In APA Style

Kien Hunter

Eastern Michigan University

Abstract

It is surreal when you think about all the ways that your computer can become a victim of a cyber invader. There are multiple methods that can be used to invade your computer while online. Most times, you will not even realize that your computer's security has been compromised until it is too late. The individuals who find their way into your computers are smart, cunning, and resourceful. Oftentimes these con artists will even use your own weaknesses against you. These individuals are coarsely known as hackers. They have the ability to plant their own tools into your system to make your computer "their" computer, trick you into giving them sensitive information, or even stop you from getting on the internet altogether. You do not have to work at a large company to be targeted for these criminal acts either, sometimes you are just in the wrong place at the wrong time. These cyber attackers take away safety, security, and peace of mind. What's scary is that no matter how well you doctor up your computer with software or how long you train your staff to watch for network problems, you can still be vulnerable.

Methods to Hacking

Hacking, at its roots, takes from the concept of social engineering. The two terms are two peas in the same pod because social engineering can display the mindset but hacking is the physical aspect. Social engineering, or con artist, is a concept that gets information from an individual (usually confidential information) either without them knowing about it, or making them feel comfortable enough to give the information out. The social engineer could choose to get quick information from individuals, or they could decide to take the longer road and study the entity that is being targeted and possibly get more refined and more useful information. It all depends on what method and how much time the hacker has to devote to it.

Social engineering can be particularly effective for gathering bits of information a little at a time. While hackers could social engineer people without knowing anything about them, the company they work for, or the type of job they do, studying a target before trying to social engineer anyone will likely gather much more useful information (Wang, 2006, 32).

Freestone and Mitchell believed that the concept of chronology plays a big role (Freestone & Mitchell, 2004). Their study showed that younger generations are not as affected by non ethical behavior on the internet because that is how they are communicating with their peers. Younger generations use the internet and technology for all aspects of life. The situation is similar to a child watching violence on television, after watching so much, it can stop becoming so gruesome. If stealing from somebody in a face-to-face environment is bad, then acquiring different forms of information and data online does not make it better just because the act is done in anonymity.

A big part of social engineering is gaining the individuals trust. If the person is being targeted but the facade of the hacker makes them comfortable, then they might overlook clues that they might notice otherwise. This is not to say that if you are conscious of everybody you talk to that you will be able to catch somebody trying to take your information but being aware is the best way to fight back. "The key to social engineering is to gain the trust of others. This is often accomplished by acknowledging, rather than questioning the targets position or authority and developing a rapport with the target" (Wang, 2006, 32). Being a social engineer, you do not to go inside of somebody's computer and steal information or invade their privacy to be a good invader. Loch, Carr, and Warkentin (1992) made a statement that gives a very good chronological timeline of how society feels about security.

Security once meant safe storage of materials, equipment, and money. Today the primary threat is to corporate data. The computing environment was historically controlled by a few knowledgeable professionals in a centralized batch processing mode. Physical security was of paramount importance. Today, almost unlimited access by a large knowledgeable community of end users from desktop, dial-in, and network facilities create new and extremely vulnerable environment (Michaels, 1990,p. 174)

A good example of a social engineer making somebody feel comfortable enough to give out information would be a social engineer playing the part of a customer service representative. When a customer calls a banking center because they have a problem with their account, they expect to speak to a bank representative to resolve their issues. The also expect to have confidentiality about the financial issues because if anything,

society is wary about their finances. What if you called because you needed to know about some changes in your account? Most likely, the individual handling your issue would ask you for your name and your account number. Sometimes you would even get asked your social security number. This is for verification purposes; just to make sure that “you are who you say you are.” What would happen if you gave your information to the service representative but they were not actually who they said they were. If they were a social engineer who intercepted the call to gain user information, then you would never know it. What did you just do? You just gave your account information and social security number to an individual who can use it any way that they please, and you don’t even know it.

The main concept of hacking or socially engineering a situation is looking for loopholes. With the right fault in judgment or lack of compensation, anybody can get into anywhere. Technology is run by the human element, the same element that Mitnick described as being the reason for system break-ins. Gamey also agreed with this idea. To paraphrase the selection in McDogall’s article, companies can be careless when they make changes (big or small) and that can lead to a doorway for an intruder to infiltrate. A small change would be firing an employee. Hypothetically, when a company fires a worker, they are supposed to deactivate that individual’s account, for security reasons. What happens if that individual is bitter about the issue and still has access to the network. With the right motivation and the wrong access, that employee can be a networks worst enemy. On the opposite end of the scale, a big change would be maintenance or reinstallation of equipment on the network. Sometimes companies

forget to arm their system with a security program and that could lead to open access into the heart of a company's network.

Using social engineering with computer savvy and malicious intent is a setup for destruction in the computer world. There are many ways that users, corporations and home users alike, can attempt to monitor and control the security level while on the internet. Because of the rise in internet security issues over the last decade, the market is very high for producing numerous antivirus software's and even hiring network security specialists to watch the network and make sure that nothing harmful can invade the network. Jaquith wrote, "In the early days, the telecom group typically managed the firewall in conjunction with the centralized wide-area networking group..." then continued to say, "It made sense to have centralized, specialized perimeter security organizations manage centralized, specialized perimeter security products." (Jaquith, 2007, P 46).

In the realm of hacking, you come across many types of hackers. There are also many different reasons for these hackers to practice their craft. Not all hackers are in the cyber terrorism business to bring governmental agencies to their knees. In fact, some do it just for the challenge or worse, for fun. Beaver commented in his document saying, "This is saying that you don't have to be on the financial end of a multimillion dollar company to get hacked, you could get targeted just for being on the network." (Beaver 2007, P 29). He also went on to say, "Many business owners and managers – even some network and security administrators – believe that they don't have anything that a hacker wants or that hackers can't do much damage if they break in. This couldn't be further from the truth." (Beaver,2007, P 29).

McDougall's article appeared to go well with this theme. He described it as ranging from targeted attacks, to being virtually random and discriminate. McDougall described the demeanor of hackers by calling them "adolescent joyriders. In his document, he said that some hackers committed these malicious acts just to see what they could get away with and who they could outsmart. It is not always for financial gain or to steal information. (McDougall, 1998, p 29) Depending on what the hacker intends to accomplish, the attack can vary. Keong and Melek assisted with this thought with stating that, "Public "defacement" of a web site is a favorite hacker ploy: it's often the first clue to indicate that uninvited visitors have been messing with the system. (Keong & Melek, 2000, P 39). Some you will see because they are done by individuals who want to gain recognition, but the potentially crippling ones, you might not see coming.

Anybody who has sat in front of a computer and decided to surf the internet has heard of the term 'malware'. This is any software that is used for malicious intent. Malware is a general term used to describe much software that intends to harm your computer, even though there a great many of different types. It's the umbrella that covers any type of foul computer play, but some methods of computer invasions stand in a class all their own.

A few popular terms that come to mind when users refer to computer security are viruses, Trojans, and worms. They are all harmful and potentially fatal to your computer system but are all different. If a hacker plants a worm in your system, you will most likely notice it because it uses up your system resources enough for you to think that something is wrong. This could be your computer slowing down or error messages popping up when you are not doing anything with your system. The factor that makes

them dangerous is that they multiply and replicate. Worms will self replicate until your system slows down. A virus is a step up from a worm on your computer. Viruses will self replicate, like a worm, but unlike a worm they can do serious damage to the system. In Bradley's documentation, he describes that viruses may contain various functions. Some replicate and multiply, or erase computer files. Some even look to make the computer itself non-operable. (Bradley, 2006,P 43). Directly, the Trojan is not harmful, whereas it can only pose as a vessel for worms, viruses, or other harmful systematic entities. A Trojan disguises itself as something, but inside something that is a danger to your system can be released as easily as double clicking on it.

Since typical computer users are used to the terms listed above, there are many that users do not know of. I will go over a few of them and explain what they do and why they are harmful. Basic users may notice that their computer is slowing down or they are starting to get an unusually large amount of pop-up's in their system, they would just call the malfunction a 'virus'. This is not correct because as you will see, your computer can be manipulated to do many things that it is not meant to do, and there is no static reason for it. Why your computer is "acting up"? It could be because you are under an attack by a software, program, or person of whom you are unaware of.

Aside from common terms another type of attack is using a botnet (or bot). A botnet is a computer that has been set up to relay or transfer information to a 'main' system. This information can vary from financial to personal information. This invasion usually takes place without the host computer's user having any knowledge of it. Frante clarified,

Methods to Hacking

A botnet is a network of zombie computers controlled by a single entity. The term is a portmanteau of the phrase "Robot Network". Usually, the zombies in use of a botnet are compromised computers running the Microsoft Windows operating system that have been infected with some sort of malware. (Frante, 2007).

The reason that many of the computers that are vulnerable to this are home users is because this type of attack takes advantage of the fact that not all users use firewalls or take other types of security measures to protect themselves and their computers. Many big corporations buy licenses for software to assist in protecting the employees from malicious invasions. Home users may believe that because they are not part of a huge organizations network, that they would not be targeted for an attack...which is definitely incorrect. This is not to say that because a computer is at home verses being at an office building it bound to be infiltrated, because that is not the real problem. The issue is not how much security a computer has on it; the issue is the fact that we are all human and human error makes up for however "smart" a computer is thought to be. Wozniak made a good point when he described the general idea of security by staying, "Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naivety', or ignorance come into play." (Mitnick, 2002, p. 4).

Bots are also able to do a number of other functions. The information transmission is just the tip of the iceberg. Once the zombie computer has been corrupted they can take control in other ways. Some of them are not as imposing or threatening, and basically may just seem to be annoying. Frante also said, "A secondary objective of the botnet is to find and compromise additional computers. While this is not considered a primary objective in and of itself, the expansion of the botnet via

assimilation of new computers helps it perform the primary objectives more efficiently.” (Frante, 2007). Other abilities of bots can cost the victim time, money, and grief. Once a bot has been installed inside of your computer, the hacker could use a rootkit to manipulate the date within your system. A rootkit is a tool kit for hackers. The explanation in Bradley’s text was, “A rootkit is a set of tools and utilities that a hacker can use to maintain access once they have accessed a system.” (Bradley, 2006, P 43). He can siphon password and login names without a user knowing it using this kit. Most of the time, the hacker will take measures to conceal his presence in the computer. He could do this by erasing log activity from the system log, erasing files, or a plethora of other methods.

One of the less intrusive attacks is click fraud. Click fraud occurs when a person clicks a banner or advertisement in order to increase the click rate for that ad. That person may not even show an interest in the specific ad, but it’s done to make the clicking statistics look better. This can increase the advertising revenue, but obviously it is false, and a crime. Some have even gone as far to hire people to do all the clicking for them. If a college student or a housewife is not making any income, then sitting in front of a computer clicking on ads seems like a way to make ends meet financially. Wang elaborated on this when he described the software approach to click fraud, “Rather than hire hordes of people to click banner ads, some website operators run automated programs known as autoclick software.” (Wang, 2006, P 272). This paragraph goes on to tell of how a Californian programmer was arrested for threatening Google with releasing his self made click fraud software.

The whole concept of advertising over the internet is tainted by the possibilities of this type of fraud. The reason that this is a legal issue is because the companies and organizations that engage in this act of fraud benefit from it in an unjust fashion. It goes along the premise of PPC (Pay per Click) advertising. Some advertising sites get paid every time a user clicks on a specific ad off of a website. So if you look at it from a money standpoint, if they are getting false clicks that register on the site, then they are getting money that they have not necessarily earned. This fraud can be used to make margins or quota's if the company is not meeting their mark. Or it can also be a way to falsify financial statistics while calculating a financial report.

Several years ago, Martin Fleischmann was a victim of click fraud. He started website www.mostchoice.com and chose to do much of his advertisement for his site using other online sites. Mostchoice.com is a site that specializes in financial services, such as mortgages and insurance issues. He was paying sites to advertise his site, but did not know that he was paying more than he owed. The article states that he paid Yahoo and Google \$2 million in advertising fees (combined). Martin was under the impression that you pay for all the clicks on his ads from prospective customers. He began registering locations that did not even advertise his site.

Now, Fleischmann's faith has been shaken. Over the past three years, he has noticed a growing number of puzzling clicks coming from such places as Botswana, Mongolia, and Syria. This seemed strange, since MostChoice steers customers to insurance and mortgage brokers only in the U.S. Fleischmann, who has an economics degree from Yale University and an MBA from Wharton, has used specially designed software to discover that the MostChoice ads being

Methods to Hacking

clicked from distant shores had appeared not on pages of Google or Yahoo but on curious Web sites with names like insurance1472.com and insurance060.com. He smelled a swindle, and he calculates it has cost his business more than \$100,000 since 2003. (Business Week, 2006).

Big internet sites such as Google and Yahoo cannot catch every single incident of this kind of fraud, nor can they be blamed for it. The sites make their money off of getting paid from advertisements, so they would not promote anything that disrupts the business or the financial flow. (Business Week, 2006)

Another form of intrusion that many people know about, or have been a victim of, is spam. "Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender." (Muller, 2008) The reason that users may seem less harmful and more vexing is because the most that users would see on their end is a barrage of emails and advertisements. Email spam is prevalent because so many people have email addresses.

The spammers will try to obtain a list of email addresses and that will be the list that they start their attack on. In some cases, the spammers will subscribe to a listing (or several listings) just to get a mailing list of addresses for that site. Beaver explained that a hacker only needs a small bit of information to have enough data to begin his assault. Sometimes it's as simple as a phone list or employee calendar. (Beaver,

2007,p 66). It may only seem like you are getting a number of annoying emails that have nothing to do with what you, but spam cost money. The internet service providers have to pay for transmitting information and data, even spam. And if they have to pay for it, guess who they charge...the subscriber!

There are, of course, a multitude of antispam methods that can be used to counteract spam and help with security issues. Corporations and home users alike can purchase some type of software to assist with keeping the email systems clean. The company that I work for currently uses an online spam guard that “washes” the email multiple times (incoming and outgoing) to check for anything that could be harmful. This helps with infecting other companies so I thought that the following quote from Andrew Jaquith would fit this situation. He said, “Organizations that practice good hygiene don’t infect their neighbors and business partners.” (Jaquith, 2007, p.50). This simply states that the less you send out, the more likely that you will infect another system.

A DoS (Denial of Service) is also a very popular attack. It does not try to take sensitive or confidential information from the victim, it only seeks to annoy the user by stopping service to the user’s computer system. Denial of Service depends somewhat on your internet service provider. Erickson wrote, “Denial of services attacks that crash services are actually more similar to program exploits than network-based exploits. Often, these attacks are dependent on a poor implementation by a specific vendor.” (Erickson, 2008, P 251). On the user’s end, this will look like they are having trouble with the internet. To misinformed users, a DoS attack would only provoke a call to the internet provider; they have no idea that they have been targeted. Erickson explained better by saying,

Methods to Hacking

Systems installed with such software are commonly referred to as bots and make up what is known as a botnet. These bots wait patiently until the attacker picks a victim and decides to attack. The attacker uses a controlling program or software, and the bots simultaneously attack the victim with some form of flooding DoS attack. Not only does the large number of distributed hosts multiply the effect of the flooding, this also makes tracing the attack source much more difficult. (Erickson, 2008, P 258).

One big step up on the security invasion would be phishing. The term “phishing” comes from a reference to the word “fishing” as in baiting users for important information. Click fraud resides on the backend of the network; users do not necessarily see the result of what happens. Spam may flood the user’s accounts with unnecessary items. The difference with these examples and with phishing is that phishing will try to manipulate the users to voluntarily put out the information that the hacker is asking for. This way, the user is prompted to put in sensitive and confidential information to a site/person unbeknownst to them. Brian Krebs wrote in his article, “Most e-mail-based malware attacks and phishing campaigns designed to trick people into handing over personal and financial data generally are blasted out indiscriminately.” (Krebs, 2008). This can be done in a few ways to try to entrap the user. Since people are becoming more aware of the threats of phishing, the con artists that try to trick users are getting more selective with whom they target for their attacks. This is called ‘spear phishing’ because they are more focused on the target group. Unlike phishing, spear phishing may just target individuals who are known to be on a certain mailing list or belong to a specific bank.

The user can get an email or get an instant message that prompts them to click a link. This link will go to a (fake) site that will ask for information such as a social security number, banking information. The bad part about it is that they look and feel like a real and trustworthy site...but that is the point. The sites are designed to look like something that the user would find trustworthy or familiar so that they will not hesitate on putting their personal information where asked. The general method of this technique is always the same; it only gets more persuading.

The tone and content of phishing emails are always the same. First, they warn that users must update their account by typing in some valuable information, often a credit card number. To lend a sense of urgency, the email also threatens that the account could be suspended if action isn't taken. (Wang, 2006, P 180).

This takes advantage of how gullible some individuals can be toward warnings in their email. Wang illustrates the threats final step in saying, "Finally, the email provides a convenient link that leads to a seemingly legitimate web page where the victim can type in his credit card number. Victims enter their credit card numbers and unknowingly give the information to a con artist." (Wang, 2006,P 181).

What makes this form of cyber intrusion so dangerous, is the many methods used that can trap an individual. Lunt stated,

Phishing schemes, where thieves get people to surrender their personal information are other examples of obedience to authority. The thieves send an email, supposedly from the victim's bank, asking the victim to verify his or her

personal information. In this case, the bank is the symbol of authority that must be obeyed, even when it's not really the bank. (Lunt, 2006).

These phishing pages are in all aspects of our computer life and we don't even know it. Kay seems to have went along with Lunt's thought,

The messages may look quite authentic, featuring corporate logos and formats similar to the ones used for legitimate messages. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes. And because these e-mails look so official, up to 20% of unsuspecting recipients may respond to them, resulting in financial losses, identity theft and other fraudulent activity against them. (Kay, 2004)

One of the ways that these seemingly helpful attacks are worded is to say that something wrong with your account. Most people would be alarmed if they find out that somebody has compromised an account for financial information, when in actuality, if you give them the information they need then you will be virtually giving them permission to compromise it. A note saying that your information has been stolen or accessed unlawfully is usually followed by a statement saying that they need you to give your personal information so that they can 'verify' it is you. Typically you will get a link that you are supposed to click which will take you to a page that has spaces for all your personal information.

Engineers manipulate the look of a site to give you the illusion that you are in the real site when you are not. Lunt also said, "Many other similar scams succeed only because we lack the analytical skills to see them for what they really are. Because of

the emphasis on procedural training rather than analytical training, more and more people are becoming robots easily controlled by their collective masters. (Lunt, 2006). People perceive what they think is the “right thing” or some are so used to a certain pattern that they have no problem giving out personal information. If an individual is an online member at Comerica Bank, and they get an email from what looks like Comerica bank, they are more than likely to respond out of habit. The idea is that because the message comes from the bank, which makes it extra important and that they must respond. This is the trap that hackers set because all people are concerned with the status and wellbeing of their finances.

In Tallinn, a man was apprehended for aggressive phishing bank information. He used his tactics to acquire user’s names and passwords for their accounts. This individual had acquired account information from multiple countries, such as Britain, Germany, and Spain. These countries laws and legislation state that if he is convicted, he will get up to five years in prison. The article describes this attack as the same as if somebody was watching you type your password into a computer. It also says that there are “hacking gangs” that are seeking out computers that they can siphon sensitive information from.

The best way to counteract a potential phishing threat would be to report it. Several sites on the internet will take matters into their own hands with these types of issues. The most known site would be www.fraud.org. There you can report the site and it will be investigated for malicious intent. If you have already input your information into a site and you believe that you have been a victim of phishing, then the next best thing for you to do would be to go to the company that was mimicked in the fraudulent

act as soon as possible. For general information on how to be a safer surfer, you could go to www.consumer.gov/idtheft or contact the Federal Trade Commission.

To come to their defense, not all hackers are corrupt con artists who want to steal your information. Some, believe it or not, are helpful. There are people who hack for a living to assist in company security. These individuals are known as ethical hackers. They hack for the good of the company. According to Coffin ethical hacking is defined as, "...an unconventional service long used by companies to protect information technology assets from hostile cyber-intruders." (Coffin, 2003, p 10). The ethical hacker is the company's 'protection plan' against real threats. Coffin explains the rationale behind hiring ethical hackers when he stated, "Companies hire ethical hackers to probe their own defenses for vulnerabilities by employing the same methods that hackers, thieves, vandals and spies would use." (Coffin, 2003, P 10). This is helpful for finding flaws and eliminating them. Coffin finishes this thought by stating, "If they find any weaknesses, they report them to their clients and advise them on ways to eliminate those vulnerabilities, and increase enterprise-wide IT security." (Coffin, 2003, P 10).

In the article by McDougall, he writes about Dave Gamey, IBM, and their security measures. He also discusses some of his thoughts on the concepts and importance of ethical hacking. Gamey is a consultant that engages in penetration testing of networks. He looks for loopholes and points of failure so that the company knows how to protect itself better. McDougall described what was at stake in the situation of Gamey and his squad of ethical hackers. Gamey would save time and money, amongst other things, if they were successful in outthinking and out-planning the hackers. But on the opposite end of the spectrum, if the infiltrators were successful in breaking into the network, then

there was virtually no limit to how much could be stolen, sabotaged, or vandalized within the company's network. (McDougall, 2002, p 31). The stakes are very high, because leaving one stone unturned leaves the door open to a multitude of attacks and potential losses. The last thing that a large corporate banking company needs is somebody who stumbles onto the network, who does not belong, who has the skill to view, modify, or extract sensitive data. With the paranoia of network security, system compromising would be something that would cause a company to lose a great deal of current and potential clients. "At the same time, the potential customers of these services are worried about maintaining control of personal information that varies from credit card numbers to social security numbers and home addresses." (Palmer, 2001, p 769)

There are various tools that can be used to ethically hack. Ironically, they are the same tools that the 'bad' hackers use to gain access into systems. In McDougall's article about Gamey, Gamey described what was used in the process of ethical hacking. Basically, Gamey and his team use the same tools and utilities as the hackers do. This is useful because it illustrates that anybody, with the right training, can become a hacker. Since Gamey was contracted by IBM, they provided some of the tools, and others were provided by various hardware and software vendors. The biggest difference with the ethical hackers in this case, is that the hackers obtained written consent from the company to proceed every step of the way (McDougall, 1998, P32). Some of the tools that are used are firewalls, Trojan Horses, and password guessers. These and many more are typical utilities that are used to try to extract information, plant viruses or malicious code, and get around network barriers. Ethical hackers have

to be just as smart and resourceful as somebody who would be looking to intrude on a network.

The fact that these ethical hackers have the same tools and skills as the threats they are trying to protect against, employees can be nervous about these individuals. They are scared of what the infiltrators are capable of, so why would they not feel the same about the good hackers? Taken from Harrington's study, there were several aspects that employees were worried about when it came to putting hackers on the payroll. Looking at the surveys, many of the employees that answered these felt very uncomfortable about the idea of having these types of workers within their network, even though they are only there to improve the security environment. A few of the main concepts that left employees with an uneasy feeling were corporate espionage, fraud, and viruses/sabotage.

In conclusion, the idea of security is a shaky subject because there are just as many factors working against security as it is working for it. The idea of security does not have to deal directly with computers or technology, because it is a state of mind. Depending on how you are planning on using the information makes a big difference. For those who work to secure network, and those who strive to break down networks, the process is the same. Adams understood the concept of security when he wrote that data encryption was important in modern day society. His point of view was that it was important because currently, so much sensitive data that is being transmitted every day. This ranges from financial transfers, state secrets, and many other forms of confidential examples. (Adams, 1990, p 323). Just because somebody gains your password or your account number does not mean that they are going to do something harmful with it. As

I stated earlier, some hack just to obtain notoriety or just for fun. It's an uneasy feeling to know that no matter how much you add to your system, you can still be compromised. It makes one lose peace of mind when you look at all the information that we let float around on the network, not knowing who might be looking at it as well. It is even more disheartening when you understand that you could have even given this information out and not even know it. Somebody could be sitting on your bank account number and password right now. Given the fact that Kevin Mitnick was previously a hacker, I think that he had the best grasp of the concept of security. An opening statement from his text sums up the importances and unfortunate vulnerabilities in modern security.

The more information that is protected, the more individuals with ill intent will excel to gain this information. There is no definitive way of protecting yourself from these predators, short of taking yourself off of the network. Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended every security product and be thoroughly vigilant about proper system configuration and apply security patches. Those individuals are completely vulnerable. (Mitnick, 2002,p 4)

Methods to Hacking

Mitnick, D. Kevin & Simon, I. William (2002). The Art of Deception: controlling the Human Element of Security. Indianapolis, Indiana: Wiley Publishing Inc

Beaver, Kevin (2007). Hacking for Dummies. Indianapolis, Indiana: Wiley Publishing Inc

Erickson, Jon (2008). Hacking: The Art of Exploitation 2nd Edition San Francisco, CA: No Starch Press

Bradley, Tony (2006). Essential Computer Security: Everyone's guide to Email, Internet, and Wireless Security. Rockland, MA: Syngress Publishing Inc.

Wallace, Wang (2006). Steal This Computer Book 4.0: What They Won't Tell You About the Internet San Francisco, CA: No Starch Press

Adams, Michael (1990 November). Hacker's Heaven. *Science News*, Vol. 138. No. 21, p. 323 Retrieved September 2008, from <http://www.jstor.org.ezproxy0.ats.msu.edu/stable/3974809>

Jaquith, Andrew (2007). Security Metrics Replace Fear, Uncertainty, and Doubt. Upper Saddle River, NJ: Pearson Education

Loch, D. Karen, Carr, H. Houston, & Warkentin, E. Merrill (June 1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding *MIS Quarterly*. Vol. 16, No. 2. P. 173-186. Retrieved September 2008, from <http://www.jstor.org.ezproxy0.ats.msu.edu/stable/249574>.

Frante, Alexandro (2007). What is a Botnet? Retrieved September 2008, from Yours Daily http://www.yoursdaily.com/science_tech/what_is_a_botnet

Click Fraud: The Dark Side of Online Advertising. *Business Week* (2006) Retrieved September 2008. From http://www.businessweek.com/magazine/content/06_40/b4003001.htm

Muller, H. Scott (2008). What is Spam? Spam Abuse.net Retrieved September 2008 From <http://spam.abuse.net/overview/whatisspam.shtml>

Kay, Russell (2004). Quickstudy: Phishing. Retrieved September 2008. From <http://www.computerworld.com/securitytopics/security/story/0,10801,89096,00.html>

Krebs, Brian (2008). Spear Phishing Targets LinkedIn Users. Retrieved October 2008 *Washington Post* from http://voices.washingtonpost.com/securityfix/2008/10/spear_phishing_attacks_against.html

Lunt, George (2006). Socialism in a Capitalist Society. Retrieved September 2008. From http://www.yoursdaily.com/money/socialism_in_a_capitalist_society

Methods to Hacking

Generation Y Attitudes Towards E-ethics and Internet-related Misbehaviors.

Freestone, O.; Mitchell, V.-W. *Journal of Business Ethics* v. 54 no2 (October 2004) p. 121-8

It Takes a Thief: Ethical Hackers Test Your Defenses.

Coffin, Bill. *Risk Management* v. 50 no7 (July 2003) p. 10-12, 14

Ethical Hacking.

Palmer, C. C. *IBM Systems Journal* v. 40 no3 (2001) p. 769-80

Information Security: The Ethical Hack.

Keong, Victor.; Melek, Adel. *CA Magazine* v. 133 no1 (January/February 2000) p. 39-40+

This Hacker's for Hire.

McDougall, Bruce. *Canadian Banker* v. 105 no6 (November/December 1998) p. 31-3

Computer crime & abuse by IS Employees: Something to Worry About?

Harrington, Susan J. *Journal of Systems Management* v. 46 (March/April 1995) p. 6-11