GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

An Insight into the Hacker Mentality
Daniel J. Willman
05/06/2004

Abstract

All hackers are not the same. In order to best deal with their actions and the intent behind their actions, one must understand who they are. Many hackers are not malicious, in that they hack for the thrill of learning and to “look around”. However, others are intent upon gathering information for gain (for profit or intelligence aspects), corrupting data or denying access to the system, or to see what harm they can cause.

With this in mind, the beginning of this paper, I will go over definitions for the common terms associated with hacking and where they came from. Also, I will take on the controversial topic of putting a definition to the term hacking for the purpose of this report where I will explain that the title of a hacker does not dictate actions, whereas all other titles in reference to the actions of the hacker. I would then like to share thoughts on theories of a hacker’s motivation. In addition, I will outline some items considered to be apart of the hackers trade, both commonly and uncommonly known and possible techniques used by any such hacker. Finally, I will discuss another controversial topic, ethical hacking, based on my previous discussion on a hacker, which will result where ethical hacking is just a hacker with permission.

Defining the hacker

The first iteration of the word hacker was first used at Massachusetts Institute of Technology (MIT) in reference to dealings with a computer. It originated from the term "hack writer" who refers to a writer that keeps "hacking" away at the typewriter until he considers his piece complete. In the 1960's and 1970's the term referred to those who were very committed to perfecting their computer software (Hafner, page 11). Whereas users with malicious intent and crackers tend to be individuals who pursue activities that are un-authorized and/or illegal, the media utilizes the term “Hacker” for these actions. Netsys.com confers this allegation with the following statement.

“*Despite media mistakes, a hacker is someone that is good with systems or networks and loves working with same. A hacker can be a cracker at times, but generally hackers are technical people who pursue their work as if it were fun. Real hackers have ethics, and are not afraid of Crackers and are sometimes used to catch Crackers” (Netsys.com).*

Hacking also referred to non-computer oriented activities that involved "manipulation of a complex system". During the 1980's, the term hacker evolved

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

to describe those who were considered for computer crimes (Hafner, 11). Hackers came to be seen in a negative, rather than a positive light.

According to Robert E. Jesek's paper on the subject, it goes into several definitions based on point of reference, such as "hacker; people who enjoy using computers and exploring the information infrastructure and systems connected to it (Jasek)." and "hacker; slang term for a computer enthusiast (Jasek)." In addition, it does a great job at clarifying who looks at a Hacker for the negative connotation versus the true meaning of cracker held within the Hacker and Security Community.

Largely due to portrayals in the media, a "hacker" is now perceived as someone who intrudes upon another's computer systems to further his or her own, possibly criminal, ends (Taylor, xi). This mentality was originally described by the term "cracker", a term generally no longer in vogue (McClure, xxv).

Crackers are malicious users intent on waging an attack against a person or system. A cracker may be motivated by greed, power, or recognition. Their actions can result in stolen property (i.e. intellectual property, data, etc.), disabled systems, compromise security, negative public opinion, loss of market share, reduced profitability, and lost productivity (Tittel, chap. 2).

In addition to the other terms heard in the Security Professional world, such as attacker, red hat, black hat, script kiddies, malicious users, etc… not a single definition or term is seen in a positive light. It is my opinion is that hackers are the only ones that are upset that these label's that have been associated with their title. Since hackers from the birth of their definition to today's current observation on their social stigma, I would prefer to associate any hacker to the profession of a police officer. Police officers helps to improve the safety and well being of any economy by doing their job, but they also have the ability to enforce the law, which the average citizen takes as a negative connotation when they get cited on a violation for breaking the law. The police officer profession has been known for improving the well being of others in addition to the negative connotation of a few who have performed illegal action. In broad terms, a hacker is a computer professional whose profession dictates their title, not their actions.

For the purpose of this report, the following shall be interpreted as the definition used for the term "hacker".

*Hacker "A person who is committed to, and good with networking and programming in reference to dealing with complex computer systems."*

Therefore, all other stigma's, labels, and definition are part of the actions of a person. When anyone refers all associated labels and titles, they are referring to the actions of a hacker, were it can be a positive or negative connotation and thus referring to a hacker.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Hacking Theories

All hackers are not the same. In order to best deal with their actions and the intent behind their actions, one must understand who they are. Many hackers are not malicious, in that they hack for the thrill of learning and to "look around". However, others are intent upon gathering information for gain, data corruption or denial of access to a system. Computer crimes come in many forms, from malicious intent from simple web defacement or system compromise to the stealing of intellectual property. Many would also put electronic espionage on that list after 9/11 since organizations use the Internet as a medium to send sensitive encrypted data. With all of the possibilities of criminal activity associated with computing systems, there is a fine line as to what dictates a computer crime versus those who have permission. Without permission, an individual could be subjugated for criminal action provided substantial evidence is available to do so.

Before you can think about how the hacker with malicious intent is going to compromise a system, the best question is why? It's a ground point for the majority of the malicious hackers out there. All hackers are not the same; they differ in skill level, motivations, and methods. Obviously, the less experienced hackers are individuals that have become to be known as script kiddies, or other individuals that hide behind aliases.

Paul Taylor discussed his own views of a hacker's motivation. These motivations include compulsive programming, a thirst for knowledge, boredom, feelings of power, desire for peer recognition within the hacking community, political acts, and rebellion against perceived bureaucracy and authority (Taylor, 44-61). Also, the normal cultural associations with race, gender, age, geographic location, or social level do not exist in cyberspace (Taylor, 30), one can state that hacker culture depends upon technology, however technology is defined. Hacker culture exists within the environment of computers, with no real physicality that is comparable to other cultures (Taylor, 26).

Nicholas Chantler conducted an ethnographic study of hackers to explore how hackers are represented in the press and to determine the threat or risk hackers pose to society at large (Chantler, 3). Objectives of the study included a description of the hacker environment, identification of hacker's characteristics, a model of how hackers process information, and development of a threat/risk approach that encompasses hacker generation, limitations, and proposed methods of control (Chantler, 3). Though many of his conclusions are based upon surveys and interviews of willing to participants, care must be taken in interpreting results since a random sample was not possible (Chantler, 169).

Chantler's study identifies three types of people who hacked (Chantler, 13). The first are students, who represented 49% of hacker's of the 284 reported events. Also, 22% were criminals who have subsequently been convicted of a

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

crime, which Chantler felt as if they were performing malicious attacks mainly for monetary gain (Chantler, 12). The final group, representing 29% of the incidents, were labeled as "others". This group contained computer security specialists, system administrators, law enforcement, journalists and authors (Chantler, 12). Based on Chantler's study, he came to the conclusions that three groups seem to exist: intelligent and well educated; bright but poorly educated and often on the wrong side of the law; and those that are juvenile and inexperienced (Chantler, 62).

Chantler spent some time exploring issues of how and why hackers begin to hack. Chantler believed that the home environment was seen as a key factor (Chantler, 78). He felt that the high numbers of juvenile hackers are in single-parent homes, often referring to younger siblings, which creates the environment that pushes young hackers to "bury themselves in the PC" (Chantler, 78). Through the Internet, these hackers find friendship and support from others in similar situations. The home environment, especially in cases of dislike of step parents, may lead to attitudes of contempt and arrogance towards "the system", resulting in little respect for laws regarding illegal hacking (Chantler, 78). Chantler theorizes that an unhappy home life may lead people to hacking (Chantler, 95).

During the survey, the motivations listed by the respondents were: addiction, freedom, knowledge, recognition, self-gratification, pleasure, challenge, friendship, excitement, profit, sabotage, espionage (obtain access to restricted information), theft, and vengeance (Chantler, 89). Chantler found that 49% of the reasons that the respondents hacked was for challenge, knowledge, and pleasure. While recognition, excitement, and friendship accounted for 24% of the motivations. These motivations were seen as "positive" or "harmless" (Chantler, 89). When it comes to targeting of systems, the majority (78%) did not pursue specific targets (Chantler, 87). They predominately went to sites that had previously been exploited (Chantler, 87). Those that did target particular sites chose their targets based on the level of challenge, particular interests in technology inherent in the system or contained in it, or the thrill or "excitement" value of the site (Chantler, 87). Chantler asked if threat of detection or prosecution inhibited hackers, in which only 73% of the respondents answered the question; one was afraid of a criminal record, but the rest did not feel threatened by existing laws (Chantler, 88). Current legislation was viewed as ineffective by 91% of the respondents (Chantler, 88).

Within the survey, over 70% of the respondents wish to work in the computing industry when the finish school. Additionally 15% are interesting in investigation, intelligence, security, and police work (Chantler, 107). This might mean that a potentially large work force would be available to other organizations looking for the hacker's unique skills over the next few years. Of interest to those that might hire hackers, 41% stated that they do not use computers to hack from work; 15% stated that they did (Chantler, 108). Overall, Chantler sees hackers

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

as a very valuable resource at the forefront of computer technology (Chantler, 168). Their self-motivation and devotion to hacking could make them an important asset to governments or corporations that require high levels of computer skills. The drawbacks are limiting a hacker's curiosity about forbidden systems, and the small (according to Chantler) number of hackers without the ethical background to determine right from wrong (Chantler, 168).

Past acts of hacking can be used to explore characteristics of hackers, which can be obtained from the evidence they leave behind. While novice hacker (i.e. script kiddies) may provide the majority of data, it is the malicious hackers that are of interest. In order to secure systems against attacks, information system security must focus on several areas. These include confidentiality, protection from computer viruses and other efforts to deny service, integrity that protects from alteration or destruction of data, and providing availability of a high level of confidence that data exchanges are only between approved and authorized users. Data encryption, access controls, data authentication, digital signatures, logging facilities and Internet security protocols are all tools to increase security within a company.

Another aspect of understanding a hacker's motivation is to understand what is going to be protected against the above said types of motivations. Therefore, the type of business is an important factor in securing systems. For example, Company A uses external web resources for financial transaction while Company B provides once a day updates to a free public website. Part of Company A might approach security by utilizing encryption, secure logins, and heavy monitoring. Company B would use different strategies that might include read only media that contains the web pages where if anything happened to the website, Company B would just reboot and reload. In both analogies, a risk management assessment should have been able to present several solutions that might work for both companies, but the type of data and/or services being protected dictates which security approach to take.

With the type of data and/or services provided by a company, there is also the likelihood of being a target (Collins, 2.2). Security Firms, High profile media targets, websites, always connected broadband connections, and dialup connections have the highest to lowest risk (Collins, 2.2). Therefore, depending on the motivation of any said "Hacker" and the type of data being protected dictates the approach to security that will be implemented into any situation. Where the type of data and services being protection in addition to a hacker's motivation should be important factors when ever performing a risk analysis.

Hacker Motivation

Many authors on hackers discuss a range of motivations for hacking. These motivations can apply together in groups or individually for each hacker. Some motivations may change over time. Taylor discussed boredom with school

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

as a motivation for hacking (Taylor, 52). When a hacker moves on to college, this motivation might diminish.

Several common personality characteristics emerge as being common to hackers. Again, this may make them less useful in profiling hackers, but may provide important leverage points to influence them. First, by the nature of the task, elite hackers tend to be very detail oriented. This can be seen in the process they use to gather information on a target (McClure, xxvi; Chantler, 109). According to Chantler, elite hackers may occasionally "short-circuit" this process in the hopes that success is possible without all of the information originally deemed necessary, less skilled hackers tend to be less thorough (Chantler, 109). Taylor shortens this to just "rattling the doors" in the hopes of success, rather than planning for success (Taylor, 102).

A second characteristic of many hackers is their persistence. They spend a large amount of time and effort in order to exploit a target system. Information about the system, the information it holds, its vulnerabilities, and even what other systems it is connected to, is built over time. Only novice hackers (script kiddies) are ones who wish to appear as such, just bash at a system in the hopes of success. This is what makes DoS and DDoS attacks interesting, while they are often seen as the last ditch effort of a frustrated script kiddies, many authors are seeking to deny access to a system (McClure, 340-341).

A third characteristic is self-esteem. Chantler explored self-esteem as part of his survey of hackers. Interestingly, the level of self-esteem corresponded to skill level. Elite hackers were judged to have high self-esteem. Those of moderate skill were seen as having average or moderate self-esteem. These two groups are those that Chantler also believes to have "positive" motivations for hacking (Chantler, 126). Those with low self-esteem were also seen as having "negative" motivations (profit, vengeance, desire to cause damage) for hacking, and possessed of little skill. Elite hackers are seen as very creative, this along with persistence can be seen as a key to success (Chantler, 23).

The final characteristic that can be explored is the degree to which someone is a self-starter or a follower, which can affect how the hacker is influenced. A self-starter will continue to hack as long as they desire to do so. In most cases, the self-starters set the pace for developing new tools and techniques. Chantler sees the elite group of hackers as being the self-starter types; those with moderate skills are seen as followers (Chantler, 126). Followers will reuse past exploits as they develop their own skills.

## The Hacker Trade

The intent of this section is not to list specific types of tool a hacker might use. Such a list would be of limited practical value since these tools and techniques are constantly changing and readily available to the public. Joel

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Scambray details many of the more common tool and technique types in their book and on the related website http://www.hackingexposed.com (Scambray). Both the book and website provide a broad list of references and Internet websites. Some types of tools will be addressed since their presence can be more easily detected, and can provide information on the hacker behind the incident.

There are two basic types of tools that can be used by a hacker. Published tools that are generally available and tools that have been created by a hacker. A hacker with only limited expertise is confined to the use published tools. While more experienced hackers might use either generally available tools or their own depending upon the circumstance. An example of a published code for hackers to utilize can be found on http://www.geocities.com/sorynhack/kit.html (Invisible Evil).

Tools that have been created for specific situations are generally much harder to detect then tools that are generally available. These tools are the attacks that are rare, if ever, noticed. These tools require the high levels of skill, and generally must be tailored to target a specific system. The intent behind the tools might be to plant trojan horses, viruses, or backdoors into a system in such a way that they can be used in the future for easily launching an attack.

There are two basic techniques to hacking – unstructured and structured. Script kiddies and others of lower skill level are primarily the hackers utilizing unstructured approaches. Taylor refers to this approach as “rattling the doors” (Taylor, 102). While Joel Scambray talks of script kiddies that “throw everything they have” at a system rather than use a more formal process such as vulnerability mapping (Scambray 34). A more skilled hacker might utilize what appears to be an unstructured attack in order to blend in with script kiddies and avoid detection. The skill level of a given hacker determines how faithfully and well they follow these steps (Scambray 34). The steps in a successful hack are target acquisition and information gathering; initial access; privilege escalation; covering of tracks; and planting back doors.

Target acquisition often begins with network reconnaissance via ping sweeps (Scambray, 34). This can reduce the target number of target systems, saves time over the course of the attack, and allows the hacker to focus efforts only on active hosts. Once an active host has been identified, the hacker then tries to identify the system (Scambray, 51-52). This can be accomplished with tactics such as banner grabbing or stack fingerprinting, which can provide information such as vendor name and/or version number. Banner grabbing consists of simple tasks such as opening a telnet connection (for UNIX or Windows NT) and pressing enter a few times to see what response the target system provides (Scambray, 70). Stack fingerprinting requires a listening port on the target system, which can determine the components of the target system (Scambray, 52). These efforts used by security administrators can aid in

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

vulnerability assessments. Vulnerability mapping is the next step in target acquisition and information gathering. It is a step that script kiddies often skip. Instead, script kiddies tend to throw everything they have at a system (Scambray, 209). This explains why many script kiddies do not know why or how an exploit works.

After a hacker has compromised a system, they often install rootkits for UNIX systems and backdoor software for Windows, so that they can regain access at a future time or pass the capability on to other hackers. These tools are often hidden so well that even if part of the hacker's exploits have been detected and the vulnerabilities corrected, they are rarely found by system administrators. These types of software comprise of four tools: trojan programs, back doors, interface sniffers, and system log cleaners (Scambray, 252). A trojan program is one that pretends to perform a useful function, but also performs code in the background without the user's knowledge (Scambray, 132). Often the background code is malicious in nature. A back door is simply a method for the hacker to return undetected in the future, generally through the use of hidden files (Scambray, 438). An interface sniffer captures, interprets, and stores packets traveling in a network for later analysis (Scambray, 253). While system log cleaners does just that, clean system log files to cover the hackers tracks.

Lets not forget that the overall patience of a Hacker is a very important factor to consider. Some firewalls and intrusion detection systems, and other like software and devices usually use time based algorithms and static signatures to determine unauthorized attempts against any particular system. Even though there are system in existence that have the ability to use algorithms to learn attacking attempts dynamically, the majority of such use static algorithms or signatures and pattern matching to do so. The two quickest ways to defeat these types of systems is with delayed or time dispersed attacks and encryption in order to avoid detection. Therefore, the patient individual can spend an enormous amount of time mounting an attack against a system.

The term 'Warez' is the name given to software that is copied illegally and either sold, traded or given away across the Internet. More experience hackers write such tools for specific purposes, while the novice hacker would use the program not knowing the specific vulnerability the tool would exploit. According to search engine statistics from recent reports, the word 'Warez' is the number one term typed into most popular online search engine facilities (Collins, 6). Just as soon as a company releases its latest software product, the Warez community is already hard at work trying to crack the software's anti-copying protection. This period in time can be very short, with many cracked software titles appearing on Warez sites around the same time as the product is officially realized to the consuming public (Collins, 6).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Ethical Hacking

Ethical hackers use their knowledge to help improve system security. Upon discovering a security flaw, they do not exploit the flaw. They fully disclose all relevant information to the affected users of the systems, software companies, mailing lists, trade press or popular media. In contrast, unethical hackers gain unauthorized access to subvert systems. They privately share their knowledge of security flaws, maintain unauthorized access, and do damage to systems (Goslar 2001). The difference between an ethical hacker from a security administrator is permission in regards to penetration testing.

Ethical hacking has evolved as part of the potential solution. Ethical hacking is fixing a system by compromising it, which has a long history of achievement but it's not clear that this technique is applicable for Internet security (Goslar 2001). A security hole on one computer is not just an isolated problem as demonstrated by recent distributed denial-of-service attacks. At present ethical hacking may be one of the most effective ways to proactively plug security holes. Ethical hackers see themselves as a necessary part of a larger vanguard protecting freedom and privacy in addition to security (Goslar 2001). While security administrators and the media see them as hackers.

For ethical hacking to have value, it must be measured against a benchmark. A benchmark could be the results of a formal risk assessment, international security standards or previous ethical hacking attempts (Tittel, 2004). In principle, ethical hacking makes sense. It is a very dangerous endeavor that can be compared to inviting burglars into your home and asking them to try and steal whatever they can. Evaluating the company or person selected to perform this service is, therefore, a crucial first step to implementing ethical hacking.

When a company decides to spend money on improving their information security, it is important to make sure that the money is well spent. In this new area of business called ethical hacking, many of these businesses are set to be exploited by unscrupulous hackers. It is therefore important to perform a proper evaluation of hackers before selecting one suitable to the business. Some companies have failed while others have had great success in using ethical hacking as a means to improve information security. There are substantial benefits when using this technique, but there is also some risk involved. By using a proper evaluation process (i.e. hiring process), this risk can be reduced to an acceptable level. Even though many businesses are currently seeking ethical hacking, by definition ethical hackers are just security administrator performing penetration testing because they have permission.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

What's to Come?

Up to this point, I have discussed that a hacker is a title that does not dictate their action and that all titles associated to hacker are in fact those actions that define the type of hacker. Then the next topic of discussion included the possible motivation of a hacker and what theories associated to them. After discussing some techniques and resources used in the hackers trade, we briefly covered the subject of ethical hacking and how it shouldn't be taken light hearted for those who wish to implement it. All of the above topics have one thing in common, what direction is network security and hacking going?

Liability is also one factor that has dramatically changed. Service providers could be held liable for knowingly allowing their networks to be used as a platform for security attacks. Conversely, they could be exempt from liability if they remove such activity from their networks upon notification of its presence. For copyrights, liability is limited for service providers whose networks are used for infringing activity or to store infringing materials when the providers have no knowledge of the activity, but act expeditiously to remove such activity and materials upon obtaining such knowledge.

Additionally, training is an important aspect to the direction of network security and hacking. Any individual may engage in self-training in addition to more formal instruction. Due to the attraction hackers have for technology, most will pursue training and improved skills on their own. In this case, any change in the style of hacking may be harder to detect. Individual training is formal coursework or exercises performed at the individual level. While the majority of formal training are not meant to train hackers, they often teach hacking techniques and tools so computer security professionals can better guard against them. Which, in turn may also help develop techniques for hackers to blend in with the security professionals environment.

In conclusion, holding true to the definition of hacking, hackers will continue to do what they do best. They will use their talent to create, modify, or improve various software and networking components. In addition, hackers will penetrate systems, write malicious code, and break into systems for various motivational factors. Every year more and more computers are falling victim to hackers. As the world's dependency upon computers increases, so does the threat of the hacker. In addition, we see hacking expanding to more than just networks and systems. Today there are hackers are targeting TiVo, dish networks, Microsoft's Xbox, and many more. Add to that the rate at which new servers are put up on the Internet along with the rate of new vulnerabilities being discovered and the ease of which they may be exploited, hacking is changing with technology, motivations and the business being performed.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

Chantler, Nicholas. "The Profile of the Computer Hacker." Inter-Pact Press, May 1997.

Ed Tittel, Mike Chapple and James Michael Stewart. "CISSP: Certified Information Systems Security Professional Study Guide" Sybes 2003 (access via http://www.books24x7.com, 5 Feb. 2004).

Goslar, Martin D. "Is There Such a Thing as Ethical Hacking?" *Information Security*, August 2001.

Invisible Evil, "Hacking Kit v2.0.b." (v1.0.c Jan. 1997, v2.0.b Mar. 1997) http://www.geocities.com/sorynhack/kit.html, (10 Mar. 2004).

Joel Scambray, Stuart McClure and George Kurtz. "Hacking Exposed: Network Security Secrets and Solutions, Second Edition" Osborne / McGraw-Hill, 2001.

John Collins, "Illegal internet feature." http://www.akamarketing.com/hacker-motivation.html, (9 Mar. 2004)

Katie Hafner & John Markoff. "Cyberpunk: Outlaws and Hackers on the Computer Frontier." Simon & Schuster 1991.

Netsys.com "The Intelligent Hacker's Choice." http://www.netsys.com/cgi-bin/display_article.cgi?1142 (8 Mar. 2004)

Paul Taylor "A. Hackers: Crime in the Digital Sublime" New York NY: Routledge, 1999.

Robert E. Jasek. "Hackers, Crackers What's in a Name." http://www.newhaven.edu/california/CJ625/p5.html, (8 Mar. 2004)

*Scott Granneman*, " Googling Up Passwords." http://www.securityfocus.com/columnists/224. (11 Mar. 2004)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.