# Who are Hackers

SANS GIAC
Practical
V.1.4b
CISSP 10 Domains Certification

Joe E Howard
August 21, 2003

## Introduction

This paper will help understand Hackers as people. The term or title Hacker brings concern to the Heart of many Security Professionals. What may have started out as programmers writing short programs called “hacks” [8], harmless pranks, ungranted access, and the spirit of "don't fence me out", has now turned into serious harm done to unsuspecting systems. However in some cases, Hackers actually benefit organizations and the web by being the watch dogs. First we must know what they are by understanding them. We need to understand the culture and the different agendas within the culture. In modern terms, they are individuals or groups of individuals who by different motives, compromise the security of an organization or person. In general, they are explorers. They are exploring new territory. Some will exploit the new territory for personal gain, others will use it be benefit others. Understanding the history behind Hackers is important as well to see what direction it has taken and where it may be going in the future. Reviewing notable hackers and common intrusion methods will help the security professional understand and raise their awareness. Exploring prevention methods also will be discussed.

## What a Hacker Is

A Hacker is an individual or group of intervals who are attempting to "hack" a system or network. The term “hack” refers to a shortcut created in a program format to do a task quicker [8]. Today’s Hackers gain access and complete some type of activity that is usually not available to the person who is partisicpating in the activity. Hackers come from non-homogeneous backgrounds, thus making them unpredictable. They help us understand a wide range of philosophies, sophistication and respect for the law. All Hackers by nature understand irregardless of their goal that “Hacking” relates to an unwanted intrusion, thus making it illegal. The reasons behind hacks also vary widely.

A definite subculture exists that promotes and hides hacker identity. Although I have learned though my studies, some actually enjoy the acclaim that there adventures bring. Most all of them have code names such as Hackingwiz or Hyper Viper [4]. They consider themselves skillful with there art and often set themselves aside from virus writers. There is no definite stereotype when it comes to identifying a Hacker. They come from varied backgrounds however almost always a common thread – they are intelligent and enjoy making computers do what they want them to do.

There are 3 widely accepted classifications of Hackers that have recently emerged [9]:

- Old School Hackers who are typically more interested in intellectual data such as lines of code or analyzing systems. This group tends to be older or involved in higher education concerning computer science.
- The second types are more like delinquents who travel around the web causing problems and hacking into sites to prove their point. More recently however, they have grown in number and consist of young adolescents involved in the activity of hacking. It is considered somewhat of a cyber joyride. They wreak havoc with methods and hacks obtained from illicit sources such as web sites dedicated to hacking. With little remorse and regard for anomintiy, they are a growing problem in today's security society.
- The Third type is Professional Criminals and Crackers. People within this group are really in to hacking for financial gain. They either have the skills to access the systems they want to hack or they employee someone who does.

Within the Hacker sub culture, there is a "Hacker ethic" [9]. This is a basic set of unwritten rules that govern activities and set the direction so to speak of their intent. More importantly, it helps to justify the activities carried out by the hacker communities. Each group has a basic set of "Hacker ethics" that are followed.

Depending on your point of view, Hackers are either beneficial and a necessary component to the internet, or they are a menace. Many feel they have a duty to point out vulnerabilities and exploit them to gain attention to the problem. They feel with this type of behavior, it will draw attention to the matter and possibly improve the issue. This can work both ways however. The same tools used for the perceived good can be used to either cause harm or assist with personal gain by other people. They also drive up the cost of the internet by drawing awareness to security on the web. This is beneficial in that is helps protect the content and personal information of web users however raises the cost due to the added attention to security.

Among well-established groups and sites and include those that advocate illegal or destructive behavior include *2600 magazine - The Hacker quarterly* [2]was formed in the early 1980's mainly targeted at phone and computer hacking. Recently in the news for publishing a program that breaks the security on DVDs so they could be copied on to computers. *Cult of the Dead Cow* [2] where responsible for the "Back Orifice", which is an open-source software that allows hackers to take over a remote system. *Hackers.com* [4] promotes the healthy side of hacking by serving as a knowledge base for the hacking community. The home page states: "providing tips and tricks for successful hacking, informational resources on previous hacks, hacking projects, and cyber security, as well as functioning as a source for learning about and downloading computer hacking tools and security utilities. Hackers.com is currently expanding its contents to offer more comprehensive resources, including solutions that address the security concerns resulting from harmful hacking activities" [4]. Established in 1994, they boast assisting over 600,000 users a month [4]. Hackers.coms mission is to raise awareness though providing tools and methods of the trade to promote hacking. This obviously raises a serious paradigm among security professionals. Most are split between the usefulness of hackers and the sometimes recklessness of others. In this author's opinion, this kind of power is dangerous in the wrong hands. However, as a security professional, studying sites like this one can only help prepare for such attacks. *Defcon* [2] is a yearly convention held in Las Vegas for Hackers and interested people to come and learn about hacking and learn tools of the trade. Among the attendees are security professionals and law enforcement agencies. They attend to gain a better knowledge of the subject and to hone their skills concerning the rising trend in cyber crime and cyber terrorism. .

## History behind the subject

Hacking is probably is as old as the computer. On day one, the computer was functioning and by day 2, it was being hacked. MIT gets credit for the first computer Hackers however. A group of young computer science majors working on a Dell punch card machine [8]. The art has no international boundaries either. Hacking is alive and well in many countries. With the advent of the modern internet, hacking has flourished.

Hacking mostly started out as an isolated phenomenon. Access routes where not well established as is the case today with the internet. Home computing had not begun its big boom. Typically, people would use dial up connections to gain access to a large government, military, or corporate entities. Yet others would sit at terminals directly connected to the system they where hacking. These systems consisted of bulkily main frame style machines with tape drives [8]. Access was typically gained by hacking the minimal security attributed to the user id and password function. Now by no means is that statement trying to say it was easier in the old days. The knowledge level of the average hacker was greater then thus needing more skill and expertise. Unlike todays web society where known malisous software and methods are readily available to people with less skill however with the same desire. Many attacks where directed towards gaining access to systems that where considered inaccessible or safe. It was considered a challenge to break the security of any given system. The phone system seemed to be a popular target for hackers since at the time was the most well established network. It was not well suited to guard against hackers. Hacking was considered a technical challenge to any computer user.

Many of same types of crimes committed today existed then as well. By the early 1980's, Bank fraud, identity theft, and extortion are just a few new cyber crimes gaining notoriety. Industrial espionage has always been a threat. Gaining access to new or emerging technology from the competition or other governments was a common occurrence.

Today we are an Internet enabled world with Web Surfers, Online Shopping, and B to B systems. The advent of the desk top computer and boom in home computing has put computers into the hands of a very large populace. This has increased the playing field for hackers. Although they are dealing with a sometimes complicated computers and networks, this does work to their advantage however. The philosophies have changed as well. Many groups serve a self appointed watch dogs over the internet to help expose weakness in commonly used software or weak security systems [2]. However, just as in the beginning, many hackers use there skills for personal gain or for the gain of the organization they are attributed with such as foreign governments and terrorist groups. Using public emails systems, terrorist can communicate through emails leveraging steganography (stego) to hide the sensitivity of there messages. Data can also be hidden in images, spam, and text messages. The modern internet has allowed hackers to explore new boundaries and assist new motives. A more recent trend is towards propaganda. The practice of battling countries to hack each others web sites and deface them or bring down the site with a denial of service attack has become common. Militaries also using hacking to disable their enemies defense systems to gain an advantage over them in battle. Financial gain is a big motive for some hackers or by people who employee hackers. Financial Institutions are often targeted in an attempt to steal large sums of money by electronic means.

## Notable Hackers and Common Intrusions

As it would seem, the Hacker community is large and widespread. *Raphael Gray* is an 18-year old hacker from rural Wales who 2000 stole an estimated 26,000 credit cards numbers from a group of e-commerce web sites and posted the numbers on the internet [1, 5]. After ex-hacker Chris Davis tracked him down, he was arrested on March 23, 2000, and charged under the United Kingdom's computer crime statute. At the time, there where myriad of charges levied against him. The complexity of the crime was not clearly understood by the prosecutors who then called in a security expert to help determine the extent of the hack. When Curador (Gray's nickname) was interviewed on why he committed this crime, he wanted to point out that the several e-commerce companies' security was weak and that valuable information, such as a credit card numbers, could be obtained. He also said that they had not taken due care in protecting the information and felt consumers had a right to know. He used, then at the time, a little known flaw in certain versions of the IIS Web Server to gain access. By exploiting this flaw, he was able to obtain the data he wanted across numerous companies in a global fashion. Curador falls in to the category of young, obviously skilled but not formally educated hacker who wanted to prove a point. His case never went to trial. He was convicted of much lesser charges and given probation.

*Phonemasters* [6] was an international group who hacked into communication companies networks and caused of $1.85 million in losses. In September of 1999, they where convicted of theft, possession of unauthorized access devices and unauthorized access to a federal computers. This conviction was supported by a datatap over a computer network [6]. They had gained access to phone numbers, the FBI's national crime database and obtained credit cards numbers to pay for illicit activities. They also downloaded thousands of calling cards and sold them to the black market. They also made money selling credit reports and information concerning well know Hollywood stars. This special skill, known among hackers as "phone phreaker" [3, 6] can be a very useful when hacking phone systems. By using these phone system hacking skills, they committed these crimes for financial gain.

*Vladimir Levin* [7, 2] a Russian hacker who engineered what is considered the internets first ever bank raid. He harvested account numbers and pins via phone calls to the bank then later put them to work transferring large sums of money to St. Petersburg and then to himself. Interestingly enough, Levin admitted to leveraging the phone system to assist his criminal activity and not the Internet. He was extradited to the United States in 1997 and convicted of conspiracy to commit bank, wire, and computer fraud. He was sentenced to 3 years and ordered to pay restitution.

Examples of common intrusion methods:

*Denial of service attacks*

This common attack can target either the network system or operating system being used. They can be considered a serious federal crime under the law. During a network based attack, an unwilling target is flooded with connection requests, preventing legitimate traffic from reaching its target. The TCP half open connection method [10] is affective by consuming targeted system resources and not responding back to the initial requested connection (ack syn). The initializing system then sends another request and leaves it half open and continues this until all the resources on the responding machine are used up. Any system connected to the Internet and is using TCP network based communication is a candidate for these types of attack [10]. There currently is not a generally accepted solution other than proper router configuration and appropriate Network/Host Based Intrusion Detection configuration.

*DNS spoofing*

When a DNS server accepts and uses incorrect information, usually intended to deceive a user, this is known as DNS spoofing. This method is used to re-direct traffic such as request for web resources and emails to a target other than intended by the user. Valuable information can be obtained such as confidential data between companies or people, personal information, and credit card information as well. Proper security on the DNS server can prevent this type of activity. Running DNS expert on the DNS server can expose any known vulnerability and help close them out.

*Packet Sniffers*

Packet Sniffers are good tools designed for system admins to debug network issues. Hackers use the tool to intercept packets and read the contents of them. By nature, the Ethernet Transmission Protocol exposes packets to all machines on the network, making your packets vulnerable to sniffing. By placing the Network Interface Card (NIC) into promiscuous mode [11], it will not discard packets not intended for that machine. It will accept them silently. Valuable information can be obtained by intercepting packets and dissecting them. Detection and prevention can be accomplished by running sniffer software and monitoring its results or using SNMP monitoring. To protect data against sniffing, encryption methods and SSL connections can help render the Hackers efforts useless since they cannot decrypt the packets, thus gaining nothing.

*Social Engineering*

This method is targeted at human resources who without prior knowledge assist Hackers who are posing as users of a system. The usual product of this activity is obtaining a user id and password information or even topology of a network. Kevin Mitnick, a notorious hacker, used this procedure in many successful hacking attempts.

*Trojan Horse Programs*

This method involves sending a user an attachment in an email that appears to be something the user would like to see or use such as a game [12]. Once the user opens the attachment, the malious code is executed or staged for execution, causing harm to the users system. Another method is the posting downloadable games or tools on the internet that are Trojan horses in disguise. Most recently, the world's first wireless virus has presented itself in the form of a Trojan horse. Propagation is usually by users and can be limited to the infected machine. Education is the best prevention for this type of intrusion. Security policy around downloading files and email policy concerning attachments should be implemented and reviewed with users. Appropriate virus software installed can aid in detection as well.

*Viruses and Worms*

A virus is a small program that is attached to another program such as a spreadsheet or word processing program. When the intended program is run, the virus also runs, doing the damage it was designed to do. It then replicates itself to insure its survival. A worm is a small piece of software that uses computer networks and holes in security to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well. Prevention includes running properly configured operating systems that are designed with security in mind such as UNIX and Windows NT. If this is not possible, running a virus scan and protection program at regular intervals such as at boot up and scheduled times will help. Security policy around downloading files and email policy concerning attachments should be implemented and reviewed with resources as well.

## Prevention

Prevention can come in many forms. A strong and consistent security policy across any enterprise or organization is the best beginning. Communicating the policy and subsequent enforcement become daily tasks that need to completed. The major areas that should be evaluated and policies put in place are:

- The Company Network
- Access to all systems both internally and externally
- Email systems
- Internet/Intranet access and content
- Physical security – building, environments
- Security of the human resources
- User Id and passwords

Designing methods of audit and reporting that are automated and alert the proper resources in case of a security event will benefit the organization a great deal. Security Professionals should implement a clear method for determining access to systems. Subsequent access control methods that are defined and updated with proper authority will lead to greater confidentiality and integrity.

Implementing Defense in Depth [14] should be considered a best practice. It will do no good to protect the front door only and leave valuable data and intellectual property unprotected when the front door is compromised. This is a common issue among many organizations and should be a priority for all security professionals. All aspects of the enterprise need to be evaluated and subsequent policy and security put in place. Security should begin at any point of entry such as the Network and continue to the Web, Application, and Data Tiers. All areas need to have security in place and common practices followed for their implementation. The email system has always been a point of enter for hackers, viruses, worms, and Trojan horses. Providing updated virus detection security on this system and evaluation of all attachments leaving and coming will alleviate problems and help maintain service level agreements. Access between test systems and production should be evaluated and policy put in place to manage. While it is definitely important to empower the support team with the necessary tools and access to assist during issues and outages, it should not compromise the security policy set forward. Support teams access policy should be regularly evaluated and monitored. Regular audits of their activities should be conducted.

The Three Principles should be a priority for any security professional [14]:

- *Confidentiality*
  Protecting sensitive information such a password and data files against compromise or destruction.
- *Integrity*
  Protecting the integrity of the data and software available to the organization.
- *Availability*
  Insuring systems are available and meeting service level agreements that may be established.

Keeping systems up to date with current software and security patches is an excellent method for the prevention of attacks. Systems and Networks fall behind on maintenance in regard to security for many reasons. Companies tend to put money into what will make profit for them and tend to worry less about what will lose money for them. A well maintained audit list of implemented security software and levels is a required practice. This should be reviewed with appropriate leaders and action taken to mitigate risks created by not having updated software and systems. Implementation plans for updates with definite timelines need to be developed and followed.

Recruiting, hiring, and subsequent training of resources is an important aspect in maintaining a secure environment. Ensuring that skill sets match the environments that are implemented and then re-current training on new concepts and software are necessary steps in securing your enterprise.

Network Based Intrusion Detection systems should be considered for implementation in any organization that does business over the web or has remote access capabilities. These systems analyze raw packet data to determine if there are intrusions attempts and can be configured to alert the appropriate resources. Host Based Intrusion Detection systems are also valuable in that they can help with analysis of previous attacks and help prepare the enterprise for future attempts. Drawing a mix between Host Based and Network Based Intrusion Detection Systems is considered a best practice since it gives the best of both and can prove more cost effective.

Security should be a high priority for any organization or enterprise.  Many times security is a second thought or put off to get a product to market.  Often, the assumption is made that adequate security is already in place.  The security factor should always be reviewed with all new projects and the minimum security levels reviewed to insure they are adequate.  Policy updates should occur consistently and be reviewed periodically for effectiveness.  Exceptions to the security policy should be minimal and reviewed for risk.  A rigorous process should be in place to have an approval process for any exception to the security policy.  Plans to eliminate exceptions to the policy should accompany any request for exception and filed with the leadership of the company and security team.  These plans should include details about there proposed compliance plan and funding set aside to become compliant.  They should also be reviewed regularly to close out exceptions.  The security policies set forward should include clear and concise communication concerning these exceptions and the risk associated.

## **Summary**

By analyzing what a Hacker is, we can begin to understand the issues faced by today's security professionals.  Due to human nature, Hackers will never go away.  However, understanding how hacker attacks begin and the damage caused can only raise the awareness and benefit any organization.  Only through defense in dept [14] and raised awareness can security professionals minimize the risk.  Prevention can come in many forms however understanding that it should be a top priority for Security Professionals in an organization is a must.  Properly education on methods of prevention and consistently visiting the issue will minimize or even mitigate the risk.  Reviewing prevention methods available can assist with the issues faced today by anyone with a computer.

## References:

1. PBS Online, 2001 “Interview: Raphael Gray a.k.a Curador” **http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/curador.html**

2. PBS Online, 2001 “Who are Hackers” **http://www.pbs.org/wgbh/pages/frontline/shows/hackers/**

3. Trigaux, Robert 2000 “A history of hacking” **http://www.sptimes.com/Hackers/history.hacking.html**

4. Hackers.com, 1998 **http://hackers.com/**

5. MJ Reed Solicitors **http://www.mjreedsolicitors.co.uk/newsraphaelgray.html**

6. Hopper, D Ian, December 1999 “Large-scale phone invasion goes unnoticed by all but FBI” **http://www.signaltonoise.net/library/phonemasters.htm**

7. TLC, 2003 “Hackers Hall of Fame” **http://tlc.discovery.com/convergence/hackers/bio/bio_09.html**

8. TLC, 2003 “A Brief History of Hacking” **http://tlc.discovery.com/convergence/hackers/articles/history.html**

9. TLC, 2003 “Hacker Psych 101” **http://tlc.discovery.com/convergence/hackers/articles/psych.html**

10. Lo, Joseph Ph.D., January 2003 “Denial of Service or "Nuke" Attacks” **http://www.irchelp.org/irchelp/nuke/**

11. CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks, November 2000 **http://www.cert.org/advisories/CA-1996-21.html**

12. Lo, Joseph Ph.D., Feburary 2003 “Trojan Horse Attacks” **http://www.irchelp.org/irchelp/security/trojan.html**

13. Internet Security Systems. “Network- vs. Host-based Intrusion Detection” Atlanta, GA A Guide to Intrusion Detection Technology

14. Cole, Eric; Northcutt, S “The SANS Institute” January 2002. “Security Essentials Day 2”