MATT BENTON

COMPUTER HACKING

THE ESSENTIAL HACKING GUIDE FOR BEGINNERS

Computer Hacking

The Essential Hacking Guide for Beginners

Introduction – What is Hacking?

Hacking is the act of gaining unauthorized access to a computer system, and can include viewing or copying data, or even creating new data. Often hacking is understood to be a way of maliciously disrupting a computer system, copying information, or leaving behind a virus that destroys data.

There are many different reasons why hacking takes place, and these reasons range from wanting to disrupt a system due to ideology (so hacking as a means of protesting); wanting to gain profit for example in order to commit credit card fraud; or simply hacking for the sake of enjoyment and amusement.

There is some controversy about the definition of the word ‘ hacker ’ because those that try to prevent such breaches in security from taking place, or seek to recover lost files, can also be known as hackers. Thus, some people believe that the correct term for malicious system security breaches is in fact ‘ cracking ’ and that ‘ hacking ’ is the correct word to use for those who fight against such malicious exploitation of computer weaknesses.

However, in the popular imagination and in general conversation, the word ‘ hacker ’ is mainly understood to refer to the ‘ bad ’ method of breaking through computer security. The two processes share many common skills, as regardless of motivation (whether to steal or protect, break in to or save, computer data) the same understanding of computers is required.

Hacking is more than simply a pastime for those who are interested in technology, and more than simply an illegal activity used for personal gain and with malicious intent, although both of these motivations do make up much of hacking activity. In fact, hacking is its own subculture, and members of the community feel very strongly about their ideologies, techniques and social relationships in the computer underworld.

There are many hacking groups and conventions, such as SummerCon, DEF CON, HoHoCon, ShmooCon, BlackHat, Chaos Communication and Hacker Halted, and local hacking communities take their entries into hacking competitions very seriously. Unsurprisingly there are also numerous online groups and forums dedicated to the subject of hacking, and there is certainly a strong community spirit felt by those with similar hacking ideologies.

Furthermore, hackers are often passionate about literary depictions of the hacking community, and ardently read fictional Cyberpunk and factual hacker magazines.

This book will serve as an introduction to the world of hacking, and will provide insight into some of the key influences, ideologies, groups, concepts, and techniques of hacking.

The first chapter will consider the beginnings of hacking and the influence of the literary genre, Cyberpunk. The second chapter will look at the different types of hackers, and draw a distinction between ethical and unethical hacking. The third chapter will look at the issue of computer security, which is vital to an understanding of hacking.

The final chapter will provide an overview of the various different techniques for hacking, including automated and manual approaches as well as the importance of the cyber confidence trick known as social engineering.

Contents

Chapter 1 – Hacking and the Influence of Cyberpunk

Michael Bruce Sterling, the American science fiction author, helped establish the popular genre of Cyberpunk. Cyberpunk is a subcategory of science fiction that focuses on the role of technology in a future setting. In this literary and cinematic genre, lower-class citizens are depicted, who have access to, and a great understanding of, advanced technology.

Cyberpunk often explores the role of technology during the breakdown of social order, in which there is an oppressive government restricting and damaging the lives of the general population. Furthermore, artificial intelligence (such as robots or intelligent computers) also plays a significant part in Cyberpunk stories, and the Earth is depicted in the near future in a post-industrial dystopia (the opposite of utopia, and therefore a bleak world characterized by oppression and often social unrest.)

The impact of Cyberpunk in the present-day understanding of hacking is considerable. Science fiction is particularly effective when we can recognize our own world within the fictional representation, and with Cyberpunk we can recognize many of the concerns of the contemporary technological age. Lawrence Person (editor of the science fiction magazine *Nova Express*) describes the typical characters in Cyberpunk:

“Classic cyberpunk characters were marginalized, alienated loners who lived on the edge of society in generally dystropic futures where daily life was impacted by rapid technological change, an ubiquitous data sphere of computerized information, and invasive modification of the human body.”

To a contemporary reader, this description of Cyberpunk characters is reminiscent of how hackers are thought of in the popular imagination, and depicted in books and in films. Therefore, the interplay between Cyberpunk characters and how we view real-life hackers is considerable: in many ways our understanding of what a hacker is like is based on how Cyberpunk characters are depicted in fiction. One example of this is how in Cyberpunk the characters often live in filthy conditions, work at night and sleep all day, and do not have any social life beyond chat rooms.

In the present-day imagination when we think of hackers we will often think of a lonely adolescent boy sitting in a darkened room behind a computer screen. In fact, Michael Bruce Sterling, who was one of the first science-fiction writers who dealt with Cyberpunk, has also shown the most interest in understanding the development of hacking.

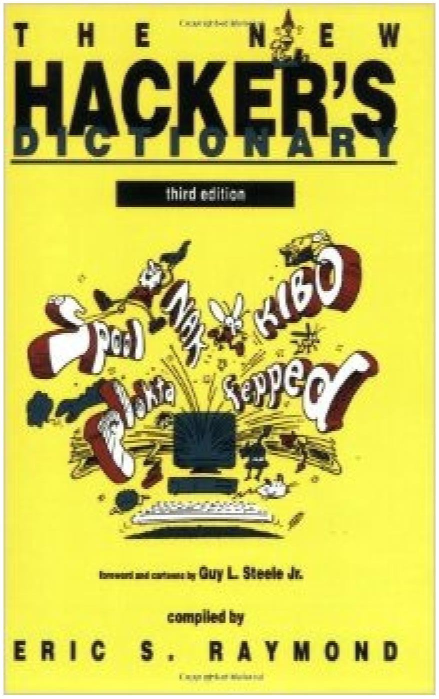
Sterling has traced the emergence of hacking, and the associated underground computer network, to the Yippies, a counterculture group who were active in the 1960s and published *Technological Assistance Program,* a newsletter that taught its readership techniques for unauthorized access to telephones, known as phreaking.

Many of the individuals who were involved in the phreaking community are also an active part of the underground hacking community, suggesting that the relationship between the two groups.

Chapter 2 – The Different Types of Hackers

The computer hacking underground contains various different subcategories of hackers. This is mainly due to conflicting ideologies, whereby certain groups calls themselves by a specific name, or call others a specific name, in order to emphasize that they do not agree with the ideologies of others.

The generic word ‘ hacker ’ therefore, although referring to those who have technical knowledge and are able to gain unauthorized access to computer systems, is rather vague and does not distinguish between those who use different methods or believe certain things.



Instead, separate names have emerged in order to distinguish between groups, and to indicate that not all hackers follow the same rules or ideologies. One way in which this can be seen, as discussed previously, is the distinction between hackers and crackers, as advocated by Eric S. Raymond in *The New Hacker ’ s Dictionary.*

In this book Raymond compiled a glossary of hackers ’ computer programming jargon, but those from the hacking community feel that this book is too biased by Raymond ’ s own view of hacking as a malicious practice.

Rather than following the dichotomy of hacker/cracker that Raymond suggested, the general hacking community feels that this is too reductive and instead advocate a wider list of name to reflect the spectrum of beliefs and practices of the large hacking community.

One subcategory of hackers is known as ‘ white hat hackers ’ and they break through computer security without a malicious motivation. Examples of why this might be done include doing so to test one ’ s own security effectiveness, or when doing work developing computer security software.

These breaches of security can occur whilst performing vulnerability assessments of computer software as part of a contractual agreement, and is therefore legal. In this way, the slang term ‘ white hat ’ references an ethical hacker who does so for positive reasons, in order to protect rather than destroy. There are recognized organizations, such as The International Council of Electronic Commerce Consultants, who provide training and certificates for this area of ethical hacking.

On the other hand, there are ‘ black hat hackers ’ who breach computer security systems simply to be malicious, or to gain profit. These hackers are the ones who are also sometimes referred to as crackers. This subcategory form the clich é hackers who are often depicted in films and television, and represent the elusive and little-understood computer criminal who the public fears.

These types of hackers violate computer security in order to destroy, change or steal information, or to prevent authorized users from being able to access the system. In this way they can cause disruption, waste time, and cause distress, but they can also steal significant amounts of money or access confidential information.

Generally a black hat hacker will spend time looking for and discovering faults in programs, or weaknesses in computer systems, but rather than alert the public to these problems they exploit them for personal gain or simply for fun. Once they have accessed a computer system, they can consequently make adjustments that prevent somebody with authorized access from using the system and thus the black hat hackers retain control.

Lying somewhere between the two, not quite a white hat hacker and not quite a black hat hacker, is the gray hat hacker. This is somebody who without being asked to searches the Internet for systems with a weakness or security flaw, and will then notify the administrator and offer to rectify the problem for a fee.

In this way they are not as good as a white hat hacker (because they are demanding a fee, and their services were never requested) but they are also not as bad as a black hat hacker because they do not exploit these weaknesses in order to wreak disruption of steal data. Another way in which gray hat hackers might respond to their discovery of a security weakness is to publish their findings online, so that the general public has access to the information.

In this way they are not performing malicious hacking themselves, but they are publishing the information, which leaves their subject at risk of a security breach. This type of hacking is illegal and also considered unethical, whether or not the gray hat hacker has breached security for personal gain, because they have gained unauthorized access to data and have left the system susceptible to hacking by malicious blat hat hacker groups.

As well as these three main classifications for hacking, which differentiate hackers based on their motivation and what they do about the information they discover, there are various other specific types of hacker. There is a social hierarchy amongst hackers, who are recognized based on their skill.

The highest of these statuses is the elite hacker, and sometimes form into elite groups such as the ‘ Masters of Deception. ’ On the other end of the scale is a script kiddie, who is still learning and has not yet developed their skills with breaching security systems. A script kiddie uses automated tool written by others, and is therefore simply following a code provided by a more skilled, black hat hacker, and not having to work it out themselves. Usually a script kiddie does not really have any knowledge or understanding of the complicated underlying technological concepts, and simply follows a plan provided by a more experienced hacker.

Even less experience than a script kiddie is a neophyte, who is a completely new hacker who has very little knowledge of computer technologies or the logic and concepts behind hacking. A blue hat refers to somebody who is used by computer security consulting firms but is not actually a part of the company; the blue hat is used to test a system prior to its launch to determine whether it has sufficient security or will be susceptible to hacking.

A hacktivist (a combination of the words ‘ hacker ’ and ‘ activist ’) is a hacker who uses their knowledge of technology and their hacking skills in order to broadcast a political, social or religious message. Hacktivism itself has two subcategories: cyber terrorism (where websites are damaged or services cannot be accessed) and freedom of information (making information available to the public that was previously either undisclosed or stored in an encrypted format.)

Groups of hackers working collectively can include organized criminal gangs, and cyber warfare of nation states. The different subcategories of hackers are indicative of the various ideologies, motivations and techniques that are present in the hacking community.

Chapter 3 – Computer Security

Before we can begin to explore the key concepts and techniques of hacking, it is helpful to first understand the basics of computer security. As hacking is the act of breaking through security measures of computer systems, an understanding of these systems is vital to any hacker who hopes to penetrate them. Computer security is applied to computers, smartphones, computer networks (public and private) and the entire Internet in order to protect devices, data and services.

Digital equipment is protected from unauthorized access by computer security, to ensure that data is not stolen, changed or deleted and to maintain the smooth running of systems. In present-day society, where digital culture forever growing, protecting these systems is extremely important and thus the field of computer security is forever growing and developing. Part of computer security is protecting the physical equipment from theft, whereas the other part of computer security is information security, to protect the data itself (and this is where hacking comes into play.)

However, sometimes these two fields overlap because if there is a breach in physical security (e.g. if a laptop is stolen) then it becomes much easier for the individual to succeed in a breach of information security, since they have the piece of equipment and it is therefore easier to access data than it is remotely.

Cyber security encompasses all security measures in place to protect a computer's data, and includes procedures such as awareness training, penetration testing, and the use of passwords to confirm authorization in order to protect data both when it is in transit and when it is simply being stored. The financial cost of being a victim of a computer security breach is considerable and as a consequence there is a lucrative market for anti-virus and computer security protection.

Computer security is a huge field because of our present-day reliance on technology. Almost every industry uses computers to a greater or lesser extent, and therefore the extent and variety of computer security measures is vast. There are some areas, however, where computer security is particularly important because they are especially vulnerable to breaches in security.

One of these is the area of financial systems, because hackers can make a profit by stealing data and consequently accessing funds. Any website that requires somebody to enter their credit card numbers are often targeted because a hacker can immediately transfer money to their own account, or spend the victim's money online.

Even if the hacker themselves do not directly use the person's bank details, they may also sell the information illegally, in order to distance themselves from the crime and attempt to avoid being caught. It is not only online that a person's data can be stolen; in-store card machines and cash points can also be rigged to collect personal information and thus gain access to funds.

People are becoming increasingly aware of this risk when doing online shopping or entering their card details, and therefore various measures are being put in place including using passwords and answering security questions. The aviation industry is another field in which computer security is of the upmost importance, because the consequences of a breach in security can range from the publication of confidential information, to the loss of expensive equipment and human life.

There are various reasons why the aviation industry may become subject to a computer security attack, depending on the motivation for the crime. These motivations include sabotage and espionage in the military aviation industry, and industrial competition and terrorism in the commercial aviation industry. Air traffic control is one of the aviation industries most vulnerable systems, because any attack can be difficult to trace, and are relatively simple because it only requires a spoof message on the radio.

There are those who seek to exploit computer vulnerabilities (either due to thrill seeking, to make a political/social statement or for financial gain) and of course on the other side those who work to uphold computer security again such threats. Somebody with knowledge of technology, and the ability to hack into computer systems, can therefore either become involved in the illegal and unethical form of hacking (otherwise known as cracking), or serve the other side by identifying threats, improving security measures and alerting companies to the vulnerabilities in their systems.

For those whose aim is to protect computer security, there are various countermeasures to guard against damaging hacking, whereby the risk of being vulnerable to a breach of computer security can be minimized or eliminated. These precautions vary in cost and complexity, but can include: intrusion detection systems (to detect threats and also analyze attacks after the event), the use of account controls (passwords and encryption of data); and the installation of firewalls (providing either hardware or software package filtering of certain forms of attack.

Precautions against a computer system being compromised by attack include making steps to prevent attack, ensure any potential attacks are detected, and the ability to respond to an attack to prevent further damage.

However, despite there being a range of countermeasures available, computer systems still remain vulnerable to attack and it is certainly not uncommon for a computer to have its security compromised. The first reason why attempted security violations still occur is that the police are often unfamiliar with computer technology and as a result do not have either the skill or the inclination to solve the crimes and apprehend the criminals responsible.

Furthermore, any investigation of such matters requires a search warrant in order for an officer to examine the entire network and this can make the procedure extremely time consuming. Another difficulty in ensuring computer security is that in the age of globalization, in which information can be shared throughout the world using the internet, and technology can spread data extremely easily, identifying and apprehending those responsible is particularly difficult.

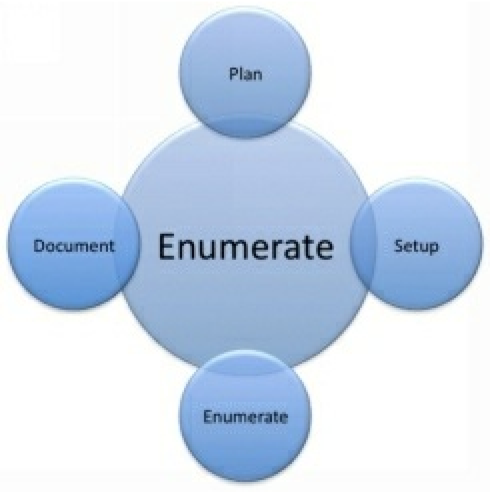
The reason for this difficulty is that a hacker might be working from one jurisdiction, while the system they are hacking into is in a different jurisdiction. Furthermore, a hacker can use various techniques (such as a temporary dial-up internet) in order to ensure their anonymity. The third problem is due to the high number of attacks that occur.

Organizations can be subject to many attacks and therefore are unable to pursue every security threat. A computer user would benefit from taking precautionary measures in order to ensure their computer security, as once a breach of security has occurred there is not much that can be done to rectify it.

Chapter 4 – Hacking Techniques

There are various techniques that can be used by hackers in order to gain unauthorized access to a computer system, in order to wreak havoc, steal money or data, or to prevent the system from operating as it is supposed to. The three main methods that are used in order to attack a system that is connected to the Internet are: network enumeration, vulnerability analysis and exploitation.

A network enumerator is a program that is used in order to discover the usernames and other information from networked computers. The program discovers any weaknesses in the computer network's security and the findings are reported to a hacker who may then use this information in order to access the network and cause damage (either by stealing data or corrupting the network.)

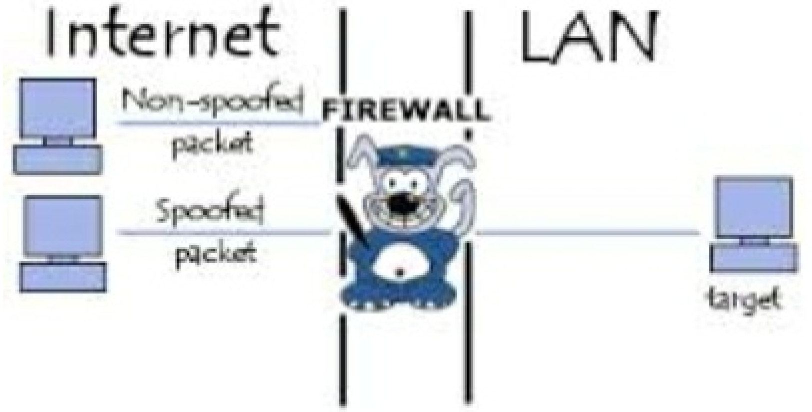


On the other hand, ethical hackers can use the same process simply to discover any weaknesses in their system in order to tighten security. Another method used is vulnerability analysis, which identifies any points of vulnerability in a system; this information can then be used to either attack the system, or to remove the weakness. Vulnerability analysis can then lead to exploitation, where the hacker uses the vulnerability information in order to breach a computer or system's security.

There are many specific techniques that can be used, but they all employ the main concepts and methods described above. The first more specific example of a hacking technique is a vulnerability scanner, which is a program used to check a network for susceptibility to attack. A port scanner can also be used, which identifies avenues of access to a computer and can establish how to circumnavigate a firewall.

As well as these mechanized devices, hackers can also find these vulnerabilities themselves, which can be done by manually searching the code of the computer and then testing whether they are right. Brute-force attack is another method by which a hacker can gain unauthorized entry to a computer network, and this involves for example guessing passwords. Password cracking is another hacking technique that uses passwords, but rather than guessing the password, the hacker recovers password information that has been stored in the computer, or transmitted.

A spoofing attack (otherwise known as phishing) is an enemy program, system or website that poses as a trusted one. By falsifying data the hacker is able to masquerade as a trusted system and thus fool a program or user into revealing confidential information such as passwords or bank details. Another hacking technique that is commonly used is a rootkit, which is a program that manages to take over the control of an operating system by employing hard to detect methods.



A Trojan horse is yet another technique that is a program which manages to fool systems and users; it works by working in one way while seeming to be doing something else. By using this method a hacker is able to gain unauthorized access to a system and create an access point so that they can re-enter via that established route later on. A computer virus is the most widely recognized form of hacking, as it is the computer threat that most of the public is aware of.

The virus works by self-replicating and implanting itself into documents and code; while some computer viruses are malicious some are merely irritating or harmless. A computer worm is similar in that it is self-replicating, but it is able to enter a computer program without a user inadvertently letting it in, and it does not need to insert itself into present programs.

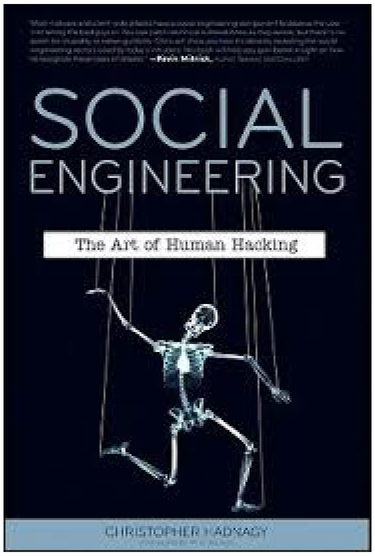
Finally, a keylogger is a tool that records every keystroke on a given machine, which can later be accessed and viewed by the hacker. This is usually to enable the hacker to access confidential information that has been typed by the victim. In fact, there are some legitimate uses for such a technique, for example some companies use a keylogger in order to detect any dishonesty or fraud committed by an employee.

A large area of computer hacking involves the use of social engineering, whereby in order to circumvent information security a person is manipulated in order to reveal confidential information or to grant access to secure networks. This technique (which includes phishing) is usually only part of a complex routine in a wider fraud scheme, but it is also a dangerous step because human beings are more likely to be won over by a convincing trickster than a machine is.

Social engineering relies on the psychological act of decision-making, and can be thought of as one of the most significant vulnerabilities in a computer security system. There are many different ways in which social engineering can be applied in order to gain unauthorized access to a computer system, and this includes criminals posing as IT technicians who pretend that they are fixing the company computers whilst in fact stealing data.

Another example would be a trickster informing a company that the number of the IT helpdesk has changed, so that when employees phone the number they will willingly disclose their account details thinking that they are talking to somebody who they can trust with the information. These sorts of scenarios come under the category of ‘pretexting’ because making up a believable scenario allows the criminal to access the required information and this leads the victim to disclose the information.

Other professionals that a hacker involved in social engineering could pose as include the police or bank manager, because these are individuals who we believe have the right to be granted any information that they request. Baiting is a subcategory of social engineering because it relies on human psychology in order to work. Baiting is where a victim’s computer security is compromised when an infected disk, device or USB stick is used.



An example of baiting would be for the criminal to post a USB through somebody’s door with a tempting sounding label and simply wait for the curious victim to plug it into their laptop, at which point malware would automatically install and infect their computer. This technique makes the most of the human tendency towards curiosity and greed, because if a label promises erotic images, money or gossip then a victim may find it hard to resist taking a look.

Kevin Mitnick, a once computer criminal who later because a security consultant, has pointed out that it is much easier and quicker to trick a person into disclosing confidential information than it is to crack into the system using luck, brute force or technical knowledge. Christopher Hadnagy has written a book titled *Social Engineering: The Art of Human Hacking, which* emphasizes the way in which humans are the most vulnerable part of any computer system.

Conclusion

This book has provided an overview of some of the key concepts to do with hacking. We have considered the beginnings of hacking and how it was influenced by the literary tradition of Cyberpunk. It is interesting to note that what was once depicted in science-fiction as an imagined activity in a dystopian society has become real and has gone on to pose a significant threat to computer security and a central concern of information technology experts.

Here we can see the true beginnings of hacking and how what was once a fictional theoretical concept has become a reality with a significant impact on the digital culture. Next we looked at the different types of hackers and noted the distinction between ethical hackers, who perform hacking legally and in order to improve computer security (otherwise known as white hat hackers) and unethical hackers, who use their skills illegally in order to wreak havoc, disrupt services, and steal information and data (otherwise known as black hat hackers.)

With this it is interesting to note how technical skill can be used differently depending on motivation, and how the hacking community is not united by a clear and consistent ideology. Subsequently we looked at computer security in order to better understand the conditions within which hacking takes place. By learning about computer security it is possible to understand the challenges faced by hackers who come up against security measures, as well as the challenges faced by those seeking to maintain the security of their computer systems.

Any introduction to hacking would not be complete without this examination of computer security because the value of maintaining computer security is what motivates ethical hackers, and what unethical hackers are fighting against. Finally we looked at the numerous different hacking techniques that can be utilized, including both automated software that finds and exploits vulnerabilities in computer systems, as well as manual methods for breaking through security measures such as discovering a password through trial and error.

In this chapter we also considered the vast area of hacking that is social engineering, by which a hacker is able to access a secure network by illegally obtaining the information needed. In today ’ s digital culture we are becoming increasingly reliant on technology for everything that we do.

As technology has improved our lives have become easier in many ways, but with this blossoming industry new types of criminals have also been created. A criminal does now not even need to leave the house in order to steal money, but can do so simply by hacking into their victim ’ s computer and accessing confidential data.

Hacking is not always illegal though, and this book has also looked at the ways in which there is an increasing demand for computer experts to become ethical hackers in order to further promote and protect computer security. This introduction to the world of hacking has revealed that hacking is not a simple activity but a huge spectrum of different behaviors that involve a wide range of techniques and motivations.

Moreover, hacking is shown to be an activity that has a strong sense of cult affiliation, in the sense that hackers strongly feel part of the hacking community. As digital culture continues to grow, it seems that both ethical and unethical hacking will become more and more skilled and its impact evermore significant.