How Hacker works

We will learn common skills hackers use to penetrate computer systems, discover hacker culture along with different types of hackers.

***TipsMake.com* - Thanks to the media, hackers have been known for their bad reputation. When it comes to the word, everyone thinks of bad guys with computer knowledge who are always looking for ways to harm people, deceive corporations, steal information and even destroy the economy or cause War by infiltrating military computer systems.** Although we cannot deny that some hackers have no malicious purpose, they still only make up a small part of the hacker community.

The term hacker computer was first used in the mid-1960s. A hacker was a programmer who hacked computer code. Hackers are able to find many different ways to use computers, create programs that no one can understand. They are the pioneers in the computer industry when building everything from small applications for the operating system. In this area, people like Bill Gates, Steve Jobs and Steve Wozniak are hackers when they can identify what the computer can do and create different ways to achieve those capabilities.

A unified way for those hackers to be knowledgeable and eager to learn. These hackers are proud of not only the ability to create new programs, but also about the ability to know how other programs and systems work. Every time a program has a bug - a technical error that makes it difficult for the program to work - hackers often create a patch - a patch to fix the problem. Some people who choose careers can improve their skills, receive money

from the software they create.

Along with the development of computers, computer programmers began to connect with each other into a system. Shortly thereafter, the term hacker meant something new - those who used computers to hack into a network they were not members of. Usually, hackers have no bad intentions. They just want to know how a computer in a network works and whether there is a barrier between them.

In fact, this still happens today. While there are many stories about bad hackers sabotaging computer systems, entering networks and spreading viruses. Most hackers are curious, they want to know all the complexities of the computer world. Some use their knowledge to help organizations and governments build a safer security system. Others may use their skills for bad purposes.

In this article, we will explore the common skills hackers use to penetrate computer systems, discover hacker culture along with different types of hackers. In addition, the article also talks about famous hackers.

Hacker rank system

According to psychologist Marc Rogers, there are some small groups of hackers like newbies, cyberpunks, coders and cyber terrorists. Newbies are unauthorized users who are not aware of how computers and programs work. Cyberpunk are knowledgeable and more difficult to detect and caught than newbie when entering the system because they tend to brag about their knowledge. Coder writes programs for other hackers to use to infiltrate the system and control computer systems. A cyber terrorist is a professional hacker who invades the system to make a profit. They can undermine the database of a company or a corporation to own important information.

For hackers above, beyond talent and understanding is code. While there is a large hacker community on the Internet, only a small number of them are actually capable of program code. Many hackers search and download code written by others. There are many different programs that hackers use to access computers and networks. These programs help hackers a lot, once they know how a system works, he can create programs to exploit that system.

Dangerous hackers often use programs to

• **Keypad lock:** Some programs help hackers get everything a computer user types on the keyboard. After being installed on the victim's computer, the program will record all the keys on the table that the user typed, providing all the information for hackers to access the system, even stealing information. someone's personal importance.

• **Password Hack** : There are many ways to steal someone's password, from password guessing to creating algorithms to combine characters, numbers and symbols. They can also use brute force attacks, which means hackers use all kinds of different combinations to be accessible. Another way is to break the password using a dictionary attack, a program capable of filling common words into a password.

• **Infecting a computer or a system with a virus:** Computer viruses are programs designed to copy themselves and cause errors such as infiltrating a computer to clean up everything on the system drive. Hackers can create a virus to infiltrate the system, but many other hackers often create a virus and send them to potential victims via email, instant messaging or websites with downloadable content or via peer network.

Gain backdoor access: Like hacked passwords, some hackers create programs to look for unprotected paths to infiltrate computers and networks. In the early days of the Internet, many computer systems did not have many

protection measures, enabling hackers to find the path to the system without needing an account and password. Another way hackers use it to infect a computer or a network is to use Trojan horse. Unlike viruses, trojans do not have self-replication function but have the same function to destroy viruses. One of the Trojan horse's traps is that it claims to help the client's machine fight the virus but instead turns it into bringing the virus into the machine.

• **Create a virtual computer:** A virtual computer is a hacker computer used to send spam or perform Distributed Denial of Service (DDoS) attacks. After the victim runs a code, the connection is opened between the victim's computer and the hacker system. Hackers can secretly control a victim's computer, use it to perform malicious purposes or distribute spam.

• **Spy on email:** Hacker has created code to help them block and read emails, almost like eavesdropping. Today, most emails are complexly encoded to prevent it unless it is blocked by a hacker, he cannot read the contents.

Culture Hacker

Phreak super

Before there were computer hackers, smart but very curious guys looking for different ways to infiltrate the telephone system, called phreaking. By phreaking, these people can make a long free call or even make a call on someone else's phone.

Many hackers are hard-to-reach people. Their most intense hobby is computers and programming that can become communication barriers. Leaving them with their own devices, a hacker can spend hours working on the computer and forgetting everything around.

The Internet has provided an opportunity for hackers to meet like-minded people. Before the Internet became easily accessible, hackers were able to set up and access bulletin board systems (BBS). A hacker can 'host' a

BBS on their computer and allow people to access the system to send messages, share information, play games and download programs. This hacker shares information for other hackers, information is shared quickly.

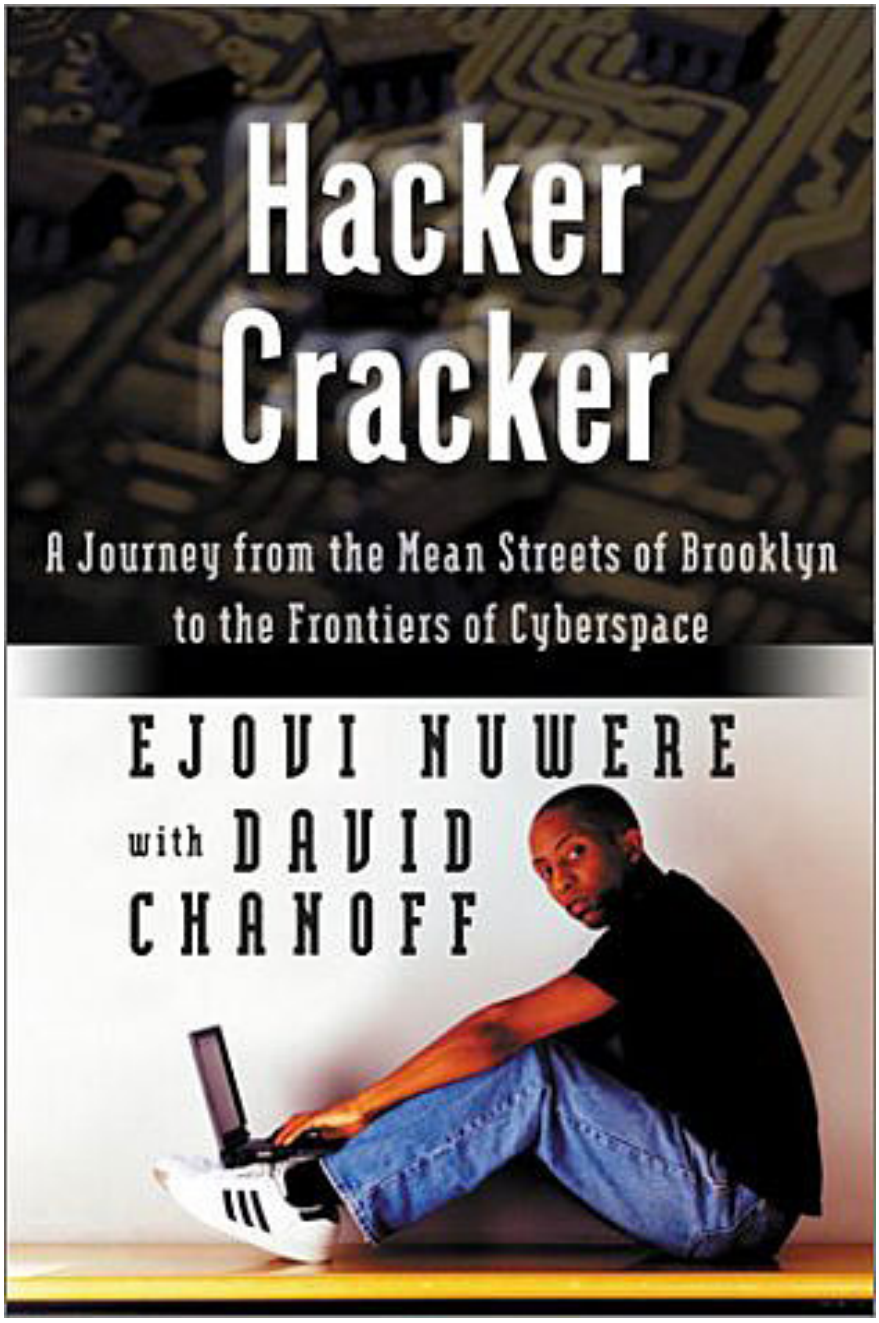
Some hackers also posted their achievements on BBS, bragging about having hacked into a security system. Usually, they will upload a document from the victim's database to prove it. In the early 1990s, the law enforcement official considered hackers a major threat to the security system. There are hundreds of people who can hack the most secure system in the world.

In addition, there are many Web sites created for hacking. Times " *2600: The Hacker Quarterly* " has reserved entries for hackers. Printed copies are still available in newspaper stalls. Other sites like Hacker.org also actively support learning, answering quizzes or organizing contests for hackers to test their skills.

When caught by law enforcement or corporations, some hackers admit that they can cause major problems. Most hackers don't want to get in trouble, instead, they hack the system just because they want to know how the system works. For a hacker, security systems like Mt. Everest, they invade just because of the absolute challenge. In the US, a hacker can get into trouble when simply entering a system. Computer abuse and fraud laws do not allow access to computer systems.

Hacker and Cracker

Many developers insist that hackers apply to people who respect the law, who create programs and apply or increase security for computers. As for anyone who uses skills with bad intentions, it is not a hacker but a cracker.



Cracker infiltrates the system and causes damage or worse. Unfortunately, most people not belonging to the hacker community are using hackers as a bad idea because they don't know how to distinguish between hackers and crackers.

Not all hackers want to access computer systems. Some people use their knowledge and intelligence to create good software, security measures. In fact, many hackers have broken into the system, then used their knowledge and ingenuity to create safer security methods. In other words, the Internet is a playground between different types of hackers - bad guys, or black hats, who are always looking for ways to illegally infiltrate systems or spread viruses and good people, or white hats, those who always strengthen the security system and develop 'killer' antivirus software.

However, hackers support both open source software and programs that source code is available for everyone to learn, copy and edit. With open source software, hackers can learn from the experiences of other hackers and

help create programs that work better than before. Programs can be simple applications to complex operating systems like Linux.

There are several hacker facts every year, mostly in support of responsible actions. A conference held annually in Las Vegas called DEFCON attracts thousands of participants to exchange software, attend debates and seminars on computer hacking and development as well as satisfy his curiosity. A similar event called Chaos Communication Camp to share software, ideas and discussions.

Hackers and laws

In general, most governments are very worried about hackers. The ability to penetrate unprotected computers, steal important information if they like, is enough for government agencies to consider it a nightmare. Secret information or intelligence is extremely important. Many government agencies do not take time to distinguish curious hackers who want to test their skills with high-end security systems and a spy.

The essays have shown this. In the US, there are a number of laws that prohibit hacking activities such as 18 USC § 1029 focusing on creating, providing and using code and devices that help hackers gain unauthorized access to a computer system. This law only records the use or creation of devices for the purpose of deception, so hackers may argue that he only uses the device to understand how a security system works.

Another important law is 18 USC § 1030, prohibiting unauthorized access to government computer systems. Even if a hacker only wants to try a system, he or she still violates the law and is penalized for not accessing government computers publicly.

The penalty depends on the level, from fine to imprisonment. A light crime also causes hackers to be imprisoned for 6 months, serious crimes can cause hackers to spend 20 years in prison. A formula from the US Justice Department's Web site is based on the economic damage caused by a hacker, along with the number of victims he or she will decide to punish the hacker.

Life hacker

Hackers who comply with the law will have a good life. Some companies have hired hackers to find errors in their security systems. Hackers can also benefit by creating utility programs and applications, just like Stanford University students Larry Page and Sergey Brin. Page and Brin worked together to create a search engine called Google. In 2008, they were ranked 26th on Forbe magazine's list of the richest people in the world.

Other countries have similar laws. Germany recently issued a law prohibiting the possession of 'hack tools'. Critics say the law is too wide and there are many legitimate applications that will be banned by the ambiguity in this law. Others think that, according to the law, companies may violate the law if they hire hackers to look for errors in the security system.

Hackers can commit criminal acts in a country when they are comfortable sitting in another country. So tracing the trail of a hacker is a complex process. Law enforcement agencies will have to contact countries to find suspects, which can take years. A famous case is the case of the US government suing hacker Gary McKinnon. McKinnon, a British hacker who successfully hacked into many military computers of the US Army and NASA, said the systems were pretty weak.

Hackers famous

Steve Jobs and Steve Wozniak, the founder of Apple, are hackers. Some of their initial actions are even similar to dangerous hacker actions. However, both Jobs and Wozniak gave up on bad deeds and focused on creating computer software and hardware. Their efforts led the way for the personal computer era - before Apple, the computer system was supposed to be the property of large corporations, very expensive and cumbersome for middle-income people.

Linus Torvalds, the father of Linux, is also a famous hacker. His open source operating system is very popular with other hackers. He helped the concept of open source software better known, showing that when you open information to people, you can harvest a lot of benefits.

Richard Stallman, often abbreviated as RMS, GNU project founder, a free operating system. He is the founder of the free software organization FSF and is against laws such as digital rights management (Digital Rights Management).

One of the other black hat hackers is Jonathan James. At the age of 16, he became the first teenage hacker to be imprisoned for stalking inside the server of the US Defense Mitigation Agency (DTRA). Jonathan deliberately installed a backdoor into the server to allow him access to sensitive emails as well as the user name and password of the employees. In addition, Jonathan attacked the US Aerospace Agency (NASA) and stole software worth $ 1.7 million. Online, he uses the nickname 'c0mrade'.

Kevin Mitnick's attention from the 1980s broke into the North American Air Defense Command (NORAD) at the age of 17. Mitnick's reputation has surfaced with his break-ins, even rumors that Mitnick has listed the FBI as the most wanted list. In everyday life, Mitnick was arrested a few times for breaking into the security system to access computer software.

Kevin Poulsen, or Dark Dante, is an expert in hacking phone systems. Kevin is famous for hacking the KIIS-FM phone server system. Poulsen's hackers act "like no one", attacking most US phone lines, upset the phone numbers recorded in Yellow Page, resulting in the phone content becoming messy. In particular, Poulsen also intervened by switching to 102 - the Porsche 944-S2 winning prize in the area's promotional program. In 1991, Poulsen was arrested, sentenced to five years in prison. At the end of his sentence, Poulsen switched to being a journalist and is currently the editor of Wired News.

Adrian Lamo hacked the computer system using computers in libraries and Internet cafes. He can hack large systems to find security holes and then use it to access the system. After that, he sent a notice to the parent company to let them know about the vulnerability. Unfortunately for Lamo, he works for hobby rather than as a hired professional and this action is illegal. In addition, he also snooped too much, read many confidential documents and accessed confidential documents. He was arrested after breaking into the popular New York Times computer system.

We can estimate that thousands of hackers work online, but a specific number is impossible. Many hackers are not aware of what they are doing - they are just using dangerous tools that they absolutely do not know. Others know what they are doing when they can go in and out of a system that nobody knows.