Table of Contents

1. Ethical Hacking – Overview

Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated.

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call **Ethical Hacking**.

A computer expert who does the act of hacking is called a "Hacker". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.

Types of Hacking

We can segregate hacking into different categories, based on what is being hacked. Here is a set of examples:

- **Website Hacking:** Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.

- **Network Hacking:** Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.

- **Email Hacking:** It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.

- **Ethical Hacking:** Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.

- **Password Hacking:** This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

- **Computer Hacking:** This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Advantages of Hacking

Hacking is quite useful in the following scenarios:

- To recover lost information, especially in case you lost your password.

- To perform penetration testing to strengthen computer and network security.

- To put adequate preventative measures in place to prevent security breaches.

- To have a computer system that prevents malicious hackers from gaining access.

Disadvantages of Hacking

Hacking is quite dangerous if it is done with harmful intent. It can cause:

- Massive security breach.
- Unauthorized system access on private information.
- Privacy violation.
- Hampering system operation.
- Denial of service attacks
- Malicious attack on the system.

Purpose of Hacking

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people indulge in hacking activities:

- Just for fun
- Show-off
- Steal important information
- Damaging the system
- Hampering privacy
- Money extortion
- System security testing
- To break policy compliance

2. Ethical Hacking – Hacker Types

Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system. These different terms come from old Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guy wears a white hat.

White Hat Hackers

White Hat hackers are also known as **Ethical Hackers**. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.

Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

Black Hat Hackers

Black Hat hackers, also known as **crackers**, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.

Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

Grey Hat Hackers

Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner’s permission or knowledge.

Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

Miscellaneous Hackers

Apart from the above well-known classes of hackers, we have the following categories of hackers based on what they hack and how they do it:

Red Hat Hackers

Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

Blue Hat Hackers

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term **BlueHat** to represent a series of security briefing events.

Elite Hackers

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

Script Kiddie

A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term **Kiddie**.

Neophyte

A neophyte, "n00b", or "newbie" or "Green Hat Hacker" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

Hacktivist

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

3. Ethical Hacking – Famous Hackers

In this chapter, we will have a brief synopsis of some of the famous Hackers and how they became famous.

Jonathan James

Jonathan James was an American hacker, ill-famous as the first juvenile sent to prison for cybercrime in United States. He committed suicide in 2008 of a self-inflicted gunshot wound.

In 1999, at the age of 16, he gained access to several computers by breaking the password of a server that belonged to NASA and stole the source code of the International Space Station among other sensitive information.

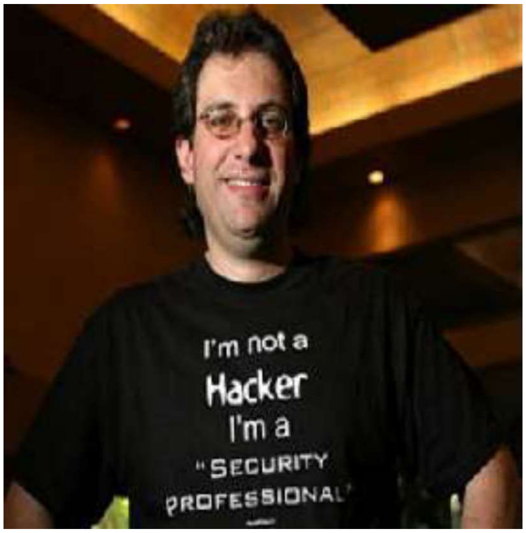
Ian Murphy

Ian Murphy, also known as Captain Zap, at one point of time was having high school students steal computer equipment for him. Ian self-proclaims to have been "the first hacker ever convicted of a crime".

Ian's career as a master hacker was fabricated in 1986 after he and his unemployed wife decided to form some type of business.

He has a long history of computer and Internet frauds. One of his favourite games is to forge Email headers and to send out third-party threat letters.

Kevin Mitnick



Kevin Mitnick is a computer security consultant and author, who infiltrates his clients' companies to expose their security strengths, weaknesses, and potential loopholes.

He is the first hacker to have his face immortalized on an FBI "Most Wanted" poster. He was formerly the most wanted computer criminal in the history of United States.

From the 1970s up until his last arrest in 1995, he skilfully bypassed corporate security safeguards, and found his way into some of the most well-guarded systems such as Sun Microsystems, Digital Equipment Corporation, Motorola, Netcom, and Nokia.

Mark Abene

Mark Abene, known around the world by his pseudonym Phiber Optik, is an information security expert and entrepreneur. He was a high-profile hacker in the 1980s and early 1990s. He was one of the first hackers to openly debate and defend the positive merits of ethical hacking as a beneficial tool to industry.

His expertise spreads across penetration studies, on-site security assessments, secure code reviews, security policy review and generation, systems and network architecture, systems administration and network management, among many others. His clientele includes American Express, UBS, First USA, Ernst & Young, KPMG and others.

Johan Helsingius

Johan Helsingius, better known as Julf, came into the limelight in the 1980s when he started operating the world's most popular anonymous remailer, called **penet.fi**.

Johan was also responsible for product development for the first Pan-European internet service provider, Eunet International.

He is at present, a member of the board of Technologia Incognita, a hackerspace association in Amsterdam, and supports the communication companies worldwide with his cyber knowledge.

Linus Torvalds

Linus Torvalds is known as one of the best hackers of all time. He rose to fame by creating Linux, the very popular Unix-based operating system. Linux is open source and thousands of developers have contributed to its Kernel. However, Torvalds remains the ultimate authority on what new code is incorporated into the standard Linux kernel. As of 2006, approximately two percent of the Linux kernel was written by Torvalds himself.

He just aspires to be simple and have fun by making the world's best operating system. Torvalds has received honorary doctorates from Stockholm University and University of Helsinki.

Robert Morris

Robert Morris, known as the creator of the Morris Worm, the first computer worm to be unleashed on the Internet. The worm had the capability to slow down computers and make them no longer usable. As a result of this, he was sentenced to three years' probation, 400 hours of community service and also had to pay a penalty amount of $10,500.

Morris is currently working as a tenured professor at the MIT Computer Science and Artificial Intelligence Laboratory.

Gary McKinnon

Gary McKinnon is a renowned systems administrator and hacker. He was famously accused of the "biggest military computer hack of all time". He had successfully hacked the networks of Army, Air Force, Navy and NASA systems of the United States government.

In his statements to the media, he has often mentioned that his motivation was only to find evidence of UFOs, antigravity technology, and the suppression of "free energy" that could potentially be useful to the public.

Kevin Poulsen

Kevin Poulsen, also known as **Dark Dante**, became famous for his notoriety when he took over all the telephone lines of Los Angeles radio station KIIS-FM, guaranteeing that he would be the 102nd caller and win the prize of a Porsche 944 S2.

Poulsen also drew the ire of FBI, when he hacked into federal computers for wiretap information, for which he had to serve a sentence of five years. He has reinvented himself as a journalist and has carved a niche for himself in this field.

4. Ethical Hacking – Terminologies

Following is a list of important terms used in the field of hacking.

- **Adware:** Adware is software designed to force pre-chosen ads to display on your system.

- **Attack:** An attack is an action that is done on a system to get its access and extract sensitive data.

- **Back door:** A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.

- **Bot:** A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.

- **Botnet:** A botnet, also known as zombie army, is a group of computers controlled without their owners' knowledge. Botnets are used to send spam or make denial of service attacks.

- **Brute force attack:** A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, over and over again, until it gets in.

- **Buffer Overflow:** Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.

- **Clone phishing:** Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.

- **Cracker:** A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.

- **Denial of service attack (DoS):** A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

- **DDoS:** Distributed denial of service attack.

- **Exploit Kit:** An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the client.