Hacker!!!...

In common usage, a hacker is a person who breaks into computers, usually by gaining access to administrative controls. The subculture that has evolved around hackers is often referred to as the computer underground. Proponents claim to be motivated by artistic and political ends, and are often unconcerned about the use of illegal means to achieve them.

Other uses of the word hacker exist that are not related to computer security (computer programmer and home computer hobbyists), but these are rarely used by the mainstream media. Some would argue that the people that are now considered hackers are not hackers, as before the media described the person who breaks into computers as a hacker there was a hacker community. This community was a community of people who had a large interest in computer programming, often sharing, without restrictions, the source code for the software they wrote. These people now refer to the cyber-criminal hackers as "crackers"

Hacker attitudes:

Based on the attitude, hackers are categorized such as white hat (ethical hacking), grey hat, black hat and script kiddie.

WHITE HAT HACKERS:

A white hat hacker, also rendered as ethical hacker, is, in the realm of information technology, a person who is ethically opposed to the abuse of computer systems. Realization that the Internet now represents human voices from around the world has made the defense of its integrity an important pastime for many. A white hat generally focuses on securing IT systems, whereas a black hat (the opposite) would like to break into them.

The term white hat hacker is also often used to describe those who attempt to break into systems or networks in order to help the owners of the system by making them aware of security flaws, or to perform some other altruistic activity. Many such people are employed by computer security companies; these professionals are sometimes called sneakers. Groups of these people are often called tiger teams.

The primary difference between white and black hat hackers is that a white hat hacker claims to observe ethical principles. Like black hats, white hats are often intimately familiar with the internal details of security systems, and can delve into obscure machine code when needed to find a solution to a tricky problem. Some use the term grey hat and fewer use brown hat to describe someone's activities that cross between black and white.

GREY HAT HACKERS:

A Grey Hat in the computer security community, refers to a skilled hacker who sometimes acts legally, sometimes in good will, and sometimes not. They are a hybrid between white and black hat hackers. They usually do not hack for personal gain or have malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits.

One reason a grey hat might consider himself to be grey is to disambiguate from the other two extremes: black and white. It might be a little misleading to say that grey hat hackers do not hack for personal gain. While they do not necessarily hack for malicious purposes, grey hats do hack for a reason, a reason which more often than not remains undisclosed. A grey hat will not necessarily notify the system admin of a penetrated system of their penetration. Such a hacker will prefer anonymity at almost all cost, carrying out their penetration undetected and then exiting said system still undetected with minimal damages. Consequently, grey hat penetrations of systems tend to be for far more passive activities such as testing, monitoring, or less destructive forms of data transfer and retrieval.

A person who breaks into a computer system and simply puts their name there whilst doing no damage can also be classified as a grey hat.

In recent years the terms white hat and black hat have been applied to the Search Engine Optimization (SEO) industry. Black hat SEO tactics, also called spamdexing, attempt unfairly to redirect search results to particular target pages, whereas white hat methods are generally approved by the search engines.

BLACK HAT HACKERS:

A black hat is a person who compromises the security of a computer system without permission from an authorized party, typically with malicious intent. The term white hat is used for a person who is ethically opposed to the abuse of computer systems, but is frequently no less skilled. The term cracker was coined by Richard Stallman to provide an alternative to using the existing word hacker for this meaning. The somewhat similar activity of defeating copy prevention devices in software which may or may not be legal in a country's laws is actually software cracking.

Use of the term "cracker" is mostly limited (as is "black hat") to some areas of the computer and security field and even there, it is considered controversial. Until the 1980s, all people with a high level of skills at computing were known as "hackers". A group that calls themselves hackers refers to "a group that consists of skilled computer enthusiasts". The other, and currently more common usage, refers to those who attempt to gain unauthorized access to computer systems. Over time, the distinction between those perceived to use such skills with social responsibility and those who used them maliciously or criminally, became perceived as an important divide. Many members of the first group attempt to convince people that intruders should be called crackers rather than hackers, but the common usage remains ingrained. The former became known as "hackers" or (within the computer security industry) as white hats, and the latter as "crackers" or "black hats". The general public tends to use the term "hackers" for both types, a source of some conflict when the word is perceived to be used incorrectly; for example Linux has been criticised as "written by hackers". In computer jargon the meaning of "hacker" can be much broader.

Usually, a black hat is a person who uses their knowledge of vulnerabilities and exploits for private gain, rather than revealing them either to the general public or the manufacturer for correction. Many black hats hack networks and web pages solely for financial gain. Black hats may seek to expand holes in systems; any attempts made to patch software are generally done to prevent others from also compromising a system they have already obtained secure control over. In the most extreme cases, black hats may work to cause damage maliciously, and/or make threats to do so as extortion.

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. These are the outcasts of the hacker community.

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. In more extreme cases, hacktivism is used as tool for Cyberterrorism. Hacktivists are also known as Neo Hackers.

Conclusion:

We have to conclude this topic by taking a strong stand against the “Cracker’s World”. Cyber crimes are increasing day by day and we have to stand against it. Each and every one should think, one of our country’s major contributions to world is in IT field, and we have the duty to protect our IT field from Cyber Terrorism. Our country has a strong growing cyber laws and apart from other laws new generations mind should mould for the completion of the cyber law. Law and judgments should be in our mind and for our mind, and the new generation must aware of it. Thank you!!