Crackers or Malicious Hackers:

System crackers attempt to access computing facilities for which they have not been authorized. Cracking a computer's defenses is seen as the ultimate victimless crime. The perception is that nobody is hurt or even endangered by a little stolen machine time. Crackers enjoy the simple challenge of trying to log in, just to see whether it can be done. Most crackers can do their harm without confronting anybody, not even making a sound. In the absence of explicit warnings not to trespass in a system, crackers infer that access is permitted. Others attack for curiosity, personal gain, or self-satisfaction. And still others enjoy causing chaos, loss, or harm. There is no common profile or motivation for these attackers.

Classification of Hackers:

Hackers can be classified broadly into three different categories:

1. Black Hat Hacker
2. White Hat Hacker
3. Grey Hat Hacker

Black Hat Hacker

Black-hat Hackers are also known as an **Unethical Hacker or a Security Cracker**. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.

White Hat Hacker

White hat Hackers are also known as **Ethical Hackers or a Penetration Tester**. White hat hackers are the good guys of the hacker world.

These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.

Gray Hat Hacker

Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.

In most cases, they tell the administrator of that system. But they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes not.

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 denialof-service attacks.

Phreaker
Phreaker is a telecom network hacker who hacks a telephone system illegally to make calls without paying for them.

State/Nation Sponsored Hackers
State or Nation sponsored hackers are those who are appointed by the government to provide them cybersecurity and to gain confidential information from other countries to stay at the top or to avoid any kind of danger to the country. They are highly paid government workers.

Malicious Insider or Whistleblower
A malicious insider or a whistleblower could be an employee of a company or a government agency with a grudge or a strategic employee who becomes aware of any illegal activities happening within the organization and can blackmail the organization for his/her personal gain.

Differences Between the Law and Ethics:

It is impossible or impractical to develop laws to describe and enforce all forms of behavior acceptable to society. Instead, society relies on **ethics** or morals to prescribe generally accepted standards of proper behavior.

Contrast of Law vs. Ethics.

Law	Ethics
Described by formal, written documents	Described by unwritten principles
Interpreted by courts	Interpreted by each individual
Established by legislatures representing all people	Presented by philosophers, religions, professional groups
Applicable to everyone	Personal choice
Priority determined by courts if two laws conflict	Priority determined by an individual if two principles conflict
Court is final arbiter of "right"	No external arbiter
Enforceable by police and courts	Limited enforcement

Assignment:

- **Describe the following terms:** Digital Signature
  Electronic Signature
  Session hijacking
  Scanning & Spoofing

- **Cyber laws to be covered as per IT Act 2008:**

  • [Section 43] Penalty and Compensation for damage to computer, computer system, etc.

  • [Section 65] Tampering with Computer Source Documents.

  • [Section 66 A] Punishment for sending offensive messages through communication service etc.

  • [Section 66 B] Punishments for dishonestly receiving stolen computer resource or communication device.

  • [Section 66C] Punishment for identity theft.

  • [Section 66D] Punishment for cheating by personation by using computer resource.

• [Section 66E] Punishment for violation of privacy.

• [Section 66F] Punishment for cyber terrorism.

• [Section 67] Punishment for publishing or transmitting obscene material in electronic form.

• [Section 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form [Section 67B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

• [Section 72] Breach of confidentiality and privacy.