BASICS OF HACKING

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose.

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Types of Hackers

Hackers are classified according to the intent of their actions. The following list classifies types of hackers according to their intent:

1. White Hat

- A "White hat" hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software.
- The term "white hat" in Internet slang refers to an **ethical hacker**.

2. Black Hat

- A "Black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain". Black hat hackers break into secure networks to destroy, modify, or steal data; or to make the network unusable for those who are authorized to use the network.
- Black hat hackers are also referred to as the **"crackers"** within the security industry and by modern programmers.

3. Grey Hat

- A grey hat hacker lies between a black hat and a white hat hacker . Grey hat hackers sometimes find the defect of a system and publish the facts to the world instead of a group of people.
- Even though grey hat hackers may not necessarily perform hacking for their personal gain, unauthorized access to a system can be considered illegal and unethical.

4. Blue Hat

- A blue hat hacker is someone outside computer security consulting films who is used to bug-test a system prior to its launch, looking for exploits so they can be closed.

5. Script kiddies

- A non-skilled person who gains access to computer systems using already made tools.

6. Hacktivist

- A hacker who uses hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.

7. Phreaker

- A hacker who identifies and exploits weaknesses in telephones instead of computers.

Cybercrime

Cybercrime is the activity of using computers and networks to perform illegal activities like spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrime hacks are committed through the internet, and some cybercrimes are performed using Mobile phones via SMS and online chatting applications.

Type of Cybercrime

The following list presents the common types of cybercrimes:

- **Computer Fraud:** Intentional deception for personal gain via the use of computer systems.
- **Privacy violation:** Exposing personal information such as email addresses, phone number, account details, etc. on social media, hacking a websites, etc.
- **Identity Theft:** Stealing personal information from somebody and impersonating that person.
- **Sharing copyrighted files/information:** This involves distributing copyright protected files such as eBooks and computer programs etc.
- **Electronic funds transfer:** This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.
- **Electronic money laundering:** This involves the use of the computer to launder money.
- **ATM Fraud:** This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.
- **Denial of Service Attacks:** This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
- **Spam:** Sending unauthorized emails. These emails usually contain advertisements.

What is Ethical Hacking?

- Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.
    - Get written permission from the owner of the computer system and/or computer network before hacking.
    - Protect the privacy of the organization been hacked.

- Transparently report all the identified weaknesses in the computer system to the organization.
- Inform hardware and software vendors of the identified weaknesses.

Why Ethical Hacking?

- Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money.
- Fake hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

Legality of Ethical Hacking

- Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking.
- The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.