Hacking: Black Hat, Grey Hat And White Hat Hackers

Introduction:

The computer has become a necessity in our daily lives where we are performing all almost all the works by sitting in the house and controlling things with the internet. There is no surprise in even saying that our lives are dependent on the internet and technology. The term internet that we are using to be online is networked to be able to surf the net. This networking makes an individual gets exposed to the external world. Protection is important when we are not alone, to able to make our data and other private information secure. In cases where the security that we are providing to our system fails, our system become vulnerable. A computer hacker is the one who is passionate about computers and how they function. To forward the computer innovation they work with other hackers and it depends on the individual whether they are using their skills for legal or illegal purposes. Purposefully gaining access to other personal systems and making them vulnerable is called Hacking.

Hacking is of two types which are Ethical hacking which is legal and Unethical hacking which is illegal. Ethical hacking is the process of locating vulnerabilities and loopholes of a computer. It serves the purpose of evaluating security and determination of any unauthorized access and any other malicious activities by taking the authorized access with the permission of the owner. Unethical hacking is a process of destroying or stealing sensitive information by using hacking tools with unintended access. In ethical hacking, the same hacking tools are used to safeguard the systems. The person who performs the activity of hacking is called hacker. Hackers have different goals according to they are doing it. Some of the goals include gaining access, hiding files, escalating privileges, deleting sensitive data, injecting malware that destroys the system and clearing tracks. Hackers are of three types.

Black Hat Hackers:

People who access computers with unauthorized access with the intention of malicious activities are called black hat hackers. These hackers are also called as unethical hackers or Black hats. These hackers mainly aim to satisfy their selfish needs by threatening the clients. Black hats, when exposed for their illegal activities, are subjected to be criminals.

White Hat Hackers:

Ethical hackers are called white hat hackers whose primary intention is to safeguard the information systems with security while working with the internet. White hats break into systems to learn about the vulnerabilities of the computer before they face massive threats. Unlike black hats, they take the permission of the client to access their system. More importantly, white hats are certified. There are different types of ethical hacking which follow the standard process to solve the issues created by black hats. Some sorts of ethical hacking are website hacking, computer hacking, network hacking, email hacking, Buffer overflow, DNS spoofing, Social engineering, wireless network hacking and DDOS. White hats only follow the given types of hacking techniques which are also used by unethical hackers to learn about the tools black hats

used, how much damage they caused, etc to protect the information systems.

Grey Hat Hackers:

Grey hats are the hackers who perform intermediate work that is performed by black hats and white hats. These hackers violate the integrity rules and standards but won't cause much damage as Black hats. The deeds that are performed by Grey hats are often considered as discernible and good.

When a system is hacked, the security of that system is at harm which is called a security threat. These threats may concern either to a computer, information system or organization. Security threats that are caused by hacking are of two types physical threats and non-physical threats. Physical threats could be internal, external or human threats like stealing a computer that contains confidential information. Non-Physical security threats are virus attacks, worms, spyware and Trojans. These threats might also include Phishing attacks and DDOS (Distributed Denial of Service). It is difficult to be attentive and protective from physical attacks whereas installing anti-viruses, smart authentication process like using strong passwords, etc. In addition to this detection of intrusion, protection of IP's and cybersecurity measures safeguards the entities from getting attacked.

There are five phases in the hacking process which are also called penetration testing stages. These are Reconnaissance, Scanning, gaining access, maintaining access, and clearing tracks respectively.

Learning about hacking and experimenting it real lives without any damage to any entity is good. In fact, helping citizens and nation by providing security promotes welfare as long as the hacking skills are not for immoral activities and selfish deeds. To become an ethical hacker one must be passionate about the hacking process and constantly educate themselves about the new methods and tools that are available. We are living in an era where society is full of unsolved issues and waiting for ethical people to solve them. In cessation helping and creating awareness about hacking is always good.