**What is Ethical Hacking?**

Ethical hacking involves the probing and testing of computer systems, networks, and applications purposely to identify and make amends on security vulnerabilities, an ethical hacker alias white-hat or pen tester, is mandated with similar goals to enhance security within an organization. The proactive approach of ethical hacking ensures the strength of organizational defenses against cyberattacks, protection of sensitive information, and compliance with security standards and regulations, this understanding and subsequent simulation of techniques used by cybercriminals make ethical hackers pivotal in maintaining a good state of cybersecurity and the protection of digital assets.

**Key aspects of ethical hacking include:**

* **Reporting**: Ethical hackers report back to the organization with the results of the tests.
* **Permission-Based**: This permission becomes necessary to differentiate their job from criminal hacking jobs
* **Objective**: The main goal is to find the holes before hostile attackers can penetrate them. This includes discovering system, application, and network vulnerabilities that an attacker could exploit.
* **Methodology**: Ethical hackers perform these steps using a variety of tools and techniques, similar to criminal hackers. It includes scanning for vulnerabilities testing to break in, and accessing control measures available.

**Importance of Ethical Hacking**

Ethical hacking contributes significantly to contemporary cybersecurity, ethical hackers are able to identify and address vulnerabilities before they are exploited by simulating the strategies and tactics utilized by cybercriminals. This proactive methodology serves to:

* **Enhance Security:** Identify and address flaws to stop data breaches and cyberattacks.
* **Compliance**: Meet security standards set by the industry and regulatory requirements.
* **Management of risk:** Assess and reduce potential threats to the assets of the organization
* **Occurrence Reaction:** Enhance the company's capacity to respond to security incidents and recover from them.

**Types of Ethical Hacking**

Depending on the focus of the security testing, ethical hacking can be broken down into a number of different categories:

* **Hacking the network:** involves testing the infrastructure of the network in order to find flaws in the protocols, configurations, and devices of the network
* **Hacking Web Applications:** Centers around distinguishing shortcomings in web applications, for example, SQL injection or cross-website prearranging (XSS) weaknesses
* **Hacking the system:** Targets working frameworks and programming to find security defects that could be taken advantage of.
* **Social Designing:** attempts to manipulate individuals into revealing confidential information or performing actions that could compromise security, putting the human element to the test.
* **Hacking into wireless networks**: involves identifying potential dangers in wireless communications and evaluating the security of wireless networks.

**Types of Ethical Hackers**

Ethical hacking is to scan vulnerabilities and to find potential threats on a computer or network. An ethical hacker finds the weak points or loopholes in a computer, web application or network and reports them to the organization. So, let’s explore more about Ethical Hacking step-by-step. These are various types of hackers:

* White Hat Hackers (Cyber-Security Hacker)
* Black Hat Hackers (Cracker)
* Gray Hat Hackers (Both)
* Blue Hat hackers
* Green Hat Hackers
* Red Hat Hackers.

Let's summarize them one by one.

1. **White Hat Hackers:** Here, we look for bugs and ethically report them to the organization. We are authorized as a user to test for bugs in a website or network and report it to them. White hat hackers generally get all the needed information about the application or network to test for, from the organization itself. They use their skills to test it before the website goes live or attacked by malicious hackers. To become a white hat hacker, you can earn a bachelor's degree in computer science, information technology, or cybersecurity. In addition, certifications such as Certified Ethical Hacker (CEH) and Certified Information Systems Security Professional (CISSP) are highly recommended.
2. **Black Hat Hackers:** Here, the organization doesn't allow the user to test it. They unethically enter inside the website and steal data from the admin panel or manipulate the data. They only focus on themselves and the advantages they will get from the personal data for personal financial gain. They can cause major damage to the company by altering the functions which lead to the loss of the company at a much higher extent. This can even lead you to extreme consequences.
3. **Grey Hat Hackers:** They sometimes access to the data and violates the law. But never have the same intention as Black hat hackers, they often operate for the common good. The main difference is that they exploit vulnerability publicly whereas white hat hackers do it privately for the company. One criticism of Grey Hat hackers is that their actions can still cause harm. Even if they do not steal or damage data, their unauthorized access to computer systems can still disrupt operations and cause financial losses for companies. Additionally, there is always the risk that a Grey Hat hacker will accidentally cause damage while attempting to identify vulnerabilities.
4. **Blue Hat hackers:**They are much like the script kiddies, are beginners in the field of hacking. If anyone makes angry a script kiddie and he/she may take revenge, then they are considered as the blue hat hackers. Blue Hat hackers payback to those who have challenged them or angry them. Like the Script Kiddies, Blue hat hackers also have no desire to learn.
5. **Green Hat hackers :**They are also amateurs in the world of hacking but they are bit different from script kiddies. They care about hacking and strive to become full-blown hackers. They are inspired by the hackers and ask them few questions about. While hackers are answering their question they will listen to its novelty.
6. **Red Hat Hackers:** They are also known as the eagle-eyed hackers. Like white hat hackers, red hat hackers also aims to halt the black hat hackers. There is a major difference in the way they operate. They become ruthless while dealing with malware actions of the black hat hackers. Red hat hacker will keep on attacking the hacker aggressively that the hacker may know it as well have to replace the whole system.