Ethical Hacking and Penetration Testing

What is Hacking?

Gaining access to a system that you are not supposed to have access is considered as hacking. For example: login into an email account that is not supposed to have access, gaining access to a remote computer that you are not supposed to have access, reading information that you are not supposed to able to read is considered as hacking. There are a large number of ways to hack a system.

In 1960, the first known event of hacking had taken place at MIT and at the same time, the term **Hacker** was organised.

What is Ethical hacking?

Ethical hacking is also known as **White hat Hacking or Penetration Testing**. Ethical hacking involves an authorised attempt to gain unauthorised access to a computer system or data. Ethical hacking is used to improve the security of the systems and networks by fixing the vulnerability found while testing.

Ethical hackers improve the security posture of an organization. Ethical hackers use the same tools, tricks, and techniques that malicious hackers used, but with the permission of the authorised person. The purpose of ethical hacking is to improve the security and to defend the systems from attacks by malicious users.

Types of Hacking

We can define hacking into different categories, based on what is being hacked. These are as follows:

1. Network Hacking
2. Website Hacking
3. Computer Hacking
4. Password Hacking
5. Email Hacking
6. **Network Hacking:** Network hacking means gathering information about a network with the intent to harm the network system and hamper its operations using the various tools like Telnet, NS lookup, Ping, Tracert, etc.
7. **Website hacking:** Website hacking means taking unauthorised access over a web server, database and make a change in the information.
8. **Computer hacking:** Computer hacking means unauthorised access to the Computer and steals the information from PC like Computer ID and password by applying hacking methods.
9. **Password hacking:** Password hacking is the process of recovering secret passwords from data that has been already stored in the computer system.
10. **Email hacking:** Email hacking means unauthorised access on an Email account and using it without the owner's permission.

Advantages of Hacking

There are various advantages of hacking:

1. It is used to recover the lost of information, especially when you lost your password.
2. It is used to perform penetration testing to increase the security of the computer and network.
3. It is used to test how good security is on your network.

Disadvantages of Hacking

There are various disadvantages of hacking:

1. It can harm the privacy of someone.
2. Hacking is illegal.
3. Criminal can use hacking to their advantage.
4. Hampering system operations.

Network Penetration Testing

Network penetration testing is the first penetration testing that we are going to cover in this section. Most of the systems and computers are connected to a network. If a device is connected to the internet, that means the device is connected to the network because the internet is a really big network. Therefore, we need to know that how devices interact with each other in a network, as well as how networks works.

Network penetration testing is divided into 3 subsections:

1. **Pre-connection attacks:** In this section, we will learn about all the attacks that we can do before connecting to a network.
2. **Gaining attacks:** In this section, we will learn that how to crack Wi-Fi keys and gain access to Wi-Fi network whether they use WEP/WPA/WPA2 network.

Post-connection attacks: These attacks apply whenever you are able to connect to the network. In this section, you will learn the number of powerful attacks that will allow you to intercept the connections and capture everything like the user-name, password, URL, chat messages. You can also modify the data as it has been sent in the air. These attacks can apply on both Wi-Fi or wired networks.