ETHICAL HACKING

By – Mandvi

In order to prevent our website, application, operating system a term 'ethical hacking' was introduced. It was first used by IBM vice president John Patrick in 1995.

A person gain access in our system and do unwanted changes in our system without our permission, is called a Hacker. He can steal data and our sensitive information.

Hackers are of three types-

1. Black Hat hacker: They do hacking without our permission in illegal way.

2. White Hat hacker: They do hacking with our permission in order to find vulnerabilities and solve them so that a black hat hacker can’t hack our device. It is ethical hacking.
3. Grey Hat hacker: They hack an device and find vulnerabilities and solve them. But they don’t take owner’s permission. In other words, they are combination of black and white hat hackers.

   By ethical hacking, we can prevent a website, application etc. from hackers.

Advantages of ethical hacking:

1. Security measures testing.
2. Identifying weak areas.
3. Understanding Hacker techniques.

4. Preparing for a hacker attack.

An ethical hacker must have following skills:

1. Proper knowledge about operating systems such as windows, LINUX, UNIX and mac.
2. Proper command on programming languages such as HTML, PHP, PYTHON, JAVASCRIPT and SQL.
3. Proper knowledge about Networking.

There are many famous institutes from where we can learn ethical hacking:

1. Indian institute of technology, Delhi.
2. Indian institute of technology, Faridabad.
3. Indian institute of electronics and technology, Chandigarh.

Some courses, we can complete for ethical hacking:

1. Certified ethical hacking by EC council.
2. Certified illusion analyst (GCIA) as an additional skill.
3. LPT, PENTEST+.
4. Cyber security expert.
5. Certified hacking forensic investigator (EC council).

It’s easy to see how businesses can benefit by using ethical hackers. A white hat hacker can reduce cyber-attack that black hat hacker would attempt to carry out using all same techniques that a real hacker would use to attack. If business defence have weakness or vulnerability, an ethical hacker can expose it so that it can be fixed before a real hack occurs.

There are some limitations in ethical hacking such as:

1. Limited scope: Ethical hackers can’t progress beyond a definite scope to make an attack successful.
2. Resources constraints: Malicious hackers don’t have time constraints that ethical hacker often face.
3. Restricted methods: Some organisations ask experts to avoid test cases that lead the servers to crash for ex. DOS attack (Denial of Service).

Ethical hackers follow key concepts such as Stay legal, Define the scope, Report vulnerabilities, Respect data sensitivity.

Ethical hacking is very useful because it helps an organisation to secure its systems from any security breach.

Thank you