Ethical Hacking

An Ethical Hacker exposes vulnerabilities in software to help business owners fix those security holes before a malicious hacker discovers them. In this free ethical hacking course, you will learn all about Ethical hacking lessons with loads of **live hacking examples** to make the subject matter clear. It is recommended you refer our Hacking Lesson/Videos sequentially, one after the other to learn how to be an ethical hacker.

What is Ethical Hacking?

Ethical Hacking is a method of identifying weaknesses in computer systems and computer networks to develop countermeasures that protect the weaknesses. An Ethical hacker must get written permission from the owner of the computer system, protect the privacy of the organization been hacked, transparently report all the identified weaknesses in the computer system to the organization, and inform hardware and software vendors of the identified weaknesses.

Types Of Hackers:
Black Hat
Grey Hat
White Hat

Black hat hackers

Black hat hackers are cybercriminals that illegally crack systems with malicious intent. Seeking to gain unauthorized access to computer systems is the definition of black hat hacking. Once a black hat hacker finds a security vulnerability, they try to exploit it

Ransomware attacks are another favored ploy that black hat hackers use to extort financial gains or breach data systems.

White hat hackers

White hat hackers are ethical security hackers who identify and fix vulnerabilities. Hacking into systems with the permission of the organizations they hack into, white hat hackers try to uncover system weaknesses in order to fix them and help strengthen a system's overall security.

Many cybersecurity leaders started out as white hat hackers, but the vital role played by ethical hacking is still widely misunderstood, as made clear by a recent ethical hacking case in Germany.(Read this article)

Gray hat hackers

Gray hat hackers may not have the criminal or malicious intent of a black hat hacker, but they also don't have the prior knowledge or consent of those whose systems they hack into. Nevertheless, when gray hat hackers uncover weaknesses such as zero-day vulnerabilities, they report them rather than fully exploiting them. But gray hat hackers may demand payment in exchange for providing full details of what they uncovered.

What's the difference between white, black, and gray hat hackers?

The main difference between white, black, and gray hat hackers is the motivation or intent that each type of hacker has when they break into computer systems. White hat hackers probe cybersecurity weaknesses to help organizations develop stronger security; black hat hackers are motivated by malicious intent; and Gray hat hackers operate in the nebulous area in between — they’re not malicious, but they’re not always ethical either.

Others Include

1. **Script Kiddies**
2. **Green Hat Hackers**
3. **Blue Hat Hackers**
4. **Red Hat Hackers**
5. **State/Nation Sponsored Hackers**
6. **Hacktivist**
7. **Malicious insider or Whistleblower**

Useful Links

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_hacker_types.htm

https://u-next.com/blogs/cyber-security/different-types-of-hackers/