Hacking and Ethics

Here I am telling you a serious truth about which many people aren't clear. Many people think ethical hacking and hacking are two different things. But in reality, an ethical hacker thinks like a malicious hacker, there is not much difference between them. In context of computer security, hacking means exploiting vulnerability in the computer system or network or software, and the person who's involved in this activity is called a hacker. And gaining access with permission and doing legal activities is called ethical hacking. The term Ethical hacking is used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, in an effort to minimize or eliminate any potential attacks.

Now I am starting a serious topic of ethics and hacking. It's mostly important to set your goal what do you want to do after learning hacking. First of all, I gonna tell you to think ethically and maintain the rule of ethics. Don't cross your limits. Don't violate any law of your country, state or company by taking part in any illegal activity.

• Maintain privacy and confidentiality of the information you gain from your professional work, (in particular as it pertains to client lists and client personal information). Do not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifiers) to a third party without client's prior consent.

• Protect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator.

• Disclose to appropriate persons' or authorities' potential dangers to any ecommerce clients, the Internet community, or the public, that you reasonably believe to be associated with a particular set or type of electronic transactions or related software or hardware.

• Never knowingly use software or process that is obtained or retained either illegally or unethically.

• Not to engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

• Use the property of a client or employer only in ways properly authorized, and with the owner's knowledge and consent.

• Disclose to all concerned parties those conflicts of interest that can't reasonably be avoided or escaped.

• Not to associate with malicious hackers and don't engage in any malicious activities.

• Ensure all penetration testing activities are authorized and within legal limits.

• Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks.

• Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities.

• Not to make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches.

• Not to be in violation of any law of the land or have any previous conviction.

Get a written permission which clearly states that you hold the authorized rights to carry out the particular test you intend for and that the said organization will back you at all times in case any criminal charges come up against you.

Always maintain formal records of what you do and what you test and what results you get. Notes can be either in paper or electronic, in all cases they must be well maintained. You're bound to gain access to private information (encryption keys for instance) while on your quest, however, how you use this information is key to being an ethical hacker and a good human being most importantly. Getting first-hand information about others' private lives doesn't give you access to intrude. Remember! There's a thin line here that must not be crossed, with great power comes great responsibility. Close out your work, not leaving anything open for you or someone else to exploit at a later time.

If you find any vulnerabilities in any software or hardware, then inform the software company or hardware manufacturer, and let them know.

And finally, I clearly state that if you do something illegal after I've warned you and you are punished by any organization, state or any country, this course won't be liable for your activities.

Be careful and stay safe.

ovidemy.com