**A complete guide to become an Ethical Hacker !**

The ethical hacker(also known as white hat hacker) is that, who discover security holes in your systems and make it secure ! The ethical hacker works like a cracker to find vulnerabilities, potential threats that could be exploited by other hackers. Remember, Attack is the best defence so always think in a hacker's way.  
  
If you are serious about your hacking career and want to become an professional ethical hacker, follow these steps:  
  
**1. Learn about computer system** :- An ethical hacker should have a good knowledge about operating systems.The Problem is most programmers are not good computer scientist. That's why vulnerabilities are found in their software. So first learn computer architecture !  If you are a windows user, then move to linux. Because linux is everywhere like server, Desktop, satellites, TV etc. Most of web server works on linux. Go to [YouTube](https://www.youtube.com/) and [google](http://www.google.co.in/" \t "_blank) for learning LINUX.I recommend you've been to use Kali-Linux.  
  
**2. Learn Programming :-** Remember, Hackers are programmers.The difference is in way of thinking only. you can be a fairly good ethical hacker without knowing any programming But people will still classify you as a script kiddie. As Many peoples don't know from where to start. I suggest you to learn HTML and python first.  There are mostly two types of hackers :    
**Computer hacker**               **Web-hacker**  
If you want to be a computer hacker, then have to learn three programming language:   
**C/C++**: Most of Operating systems are written in C/C++. it is also used for Exploit writing and development. In [Programming :  Ethical Hacker way](http://programmingethicalhackerway.blogspot.in/search/label/C) blog you'll find complete tutorials for learning C/C++ in hacker way.  
  
**Python :**Python is becoming the  natural leader in the hacking- programming language department.Python is the language of choice for hackers and security analysts for creating powerful and effective tools.it is most used language for exploit writing. In[Programming : Ethical Hacker way](http://programmingethicalhackerway.blogspot.in/search/label/Python)blog you'll find complete tutorials for learning python in hacker way.  
  
**Assembly Language :** If your computer can do something, you can write assembly code to do it. Assembly language is probably the most important things one needs to master if he/she desire to enter the world of hacking.A hacker that hasn't mastered Assembly language is not a hacker because nothing really moves without it.Reverse Engineers also uses Assembly language. In [Programming : Ethical Hacker way](http://programmingethicalhackerway.blogspot.in/search/label/Assembly) blog you'll find complete tutorials for learning Assembly in hacker way.   
  
If you want to be a web hacker, then have to learn these programming language:  
  
**HTML** : it is so easy to learn. A hacker must have basic knowledge about HTML which makes easy to understand web pages,XSS , phishing etc. When there is a  vulnerability in victim’s website, a hacker must have a little idea about what it is. Hence he must get used to HTML to identify and take control over the website!   
  
**JavaScript :** It is client-side programming language. if you want to exploit Client side vulnerabilities, then you need javascript and html knowledge.  
  
**PHP :**It is server-side programming language.it is strongly recommended to every web Penetration tester.  
A very good resource of learning PHP :  [PHP at the Core: A Hacker's Guide](http://php.net/manual/en/internals2.php)  
  
**SQL :**Structured Query Language is database programming language.Most of you heard about SQL injection. To exploit SQL injection vulnerability in websites, You must have knowledge  of  SQL programming and PHP.  
  
  
**3.Learn networking :-**An ethical hacker should have knowledge about how network operates and networking term like IP/TCP, port, protocol, router, modem and many more terms. If you want to be good in networking then you can set up your own home network. II suggest you to learn: How network work, what is TCP/IP, About Protocols and port, About OSI model. Networking helps in Developing remote exploits, Attacking network application like SMTP, FTP etc. In [Programming : Ethical Hacker way](http://programmingethicalhackerway.blogspot.in/search/label/networking)blog you'll find complete tutorials for learning networking in hacker way.  
  
**4. Join hackers forums :-** Join ethical hacking Groups on social websites like [Facebook](https://www.facebook.com/), [Twitter](https://twitter.com/) etc. Subscribe to hacker news websites. join ethical hacking communities like [HackThisSite](https://www.hackthissite.org/" \t "_blank), Black-Hat Forums etc...

[](http://3.bp.blogspot.com/-n9YqMIIcGxo/VaSnRQ2zvSI/AAAAAAAAAAM/Q8bow73XeuI/s1600/hacking.jpg)

**5. Working of an ethical hacker :-**  
  
-> Working ethically.  
-> Respecting Laws.  
-> Not harm systems.  
  
**6. Professional Ethical Hacking course :**  
  
[**CEH(certified ethical hacker)**](http://www.eccouncil.org/)**:**The Certified Ethical Hacker is a professional certification, provided by the International Council of E-Commerce Consultants (EC-Council). For more information : http://www.eccouncil.org/  
  
[**SANS Security**](http://www.sans.org/)**:** SANS is by far the largest source for information security training and security certification in the world. They offer many types of Security Training Courses. For more information http://www.sans.org/courses/  
  
[**Offensive security**](http://www.offensive-security.com/)**:**Offensive security offer many types of information security certification courses like OSCP (offensive security certified professional), OSEE(offensive security exploitation expert) etc.  
For more information : http://www.offensive-security.com/information-security-certifications/  
  
**7. Resources : Books**  
When you go to Google and search for Proper resources of learning hacking, then may be you don't get Proper resources of learning. Here i will share my hacking experience. Hope This will help you too.  
  
**For learning Hacking :**  
[**Hacking: The Art of Exploitation**](http://www.amazon.in/gp/product/1593271441/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=1593271441&linkCode=as2&tag=proethhacsway-21&linkId=YCE2I4WSLDO74VV4)**:** This is a very good book on the subject of hacking. this is one of the best technical hacking books I've read so far. it covers all of the fundamentals like Networking, Programming, shell coding, Exploitation, Cryptology which is required for every hacker in great detail.  
  
[**The Hacker's Underground Handbook :**](http://www.amazon.in/gp/product/1451550189/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=1451550189&linkCode=as2&tag=proethhacsway-21&linkId=ALW7HEZKNQZ7J3LM)If you are coming from a position of absolutely no knowledge of the hacking, this may be useful to you. This book will guide you in the right direction helping you understand password cracking,  phishing, network hacking, wireless hacking, malware, Windows hacking and etc.  
  
[**Gray Hat Hacking -The Ethical Hackers Handbook**](http://www.amazon.in/gp/product/0071077316/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=0071077316&linkCode=as2&tag=proethhacsway-21&linkId=E3VI6LFD2L2FJ2EC)**:** this book allows the reader to gain very practical knowledge around current security issues while gaining knowledge that can be applied regardless of future events.The book also covers several well known tools that every admin should be aware of for use in Hacking. The authors provide a fairly comprehensive overview of the legal and ethical implications of hacking and how to properly disclose exploit code to vendors without damaging any systems.  
  
[**Violet python -A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers:**](http://www.amazon.in/gp/product/1597499579/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=1597499579&linkCode=as2&tag=proethhacsway-21&linkId=IUCR5GU5ETBGCZMS)It is great for those who are new to the python language and would like example use cases of simplistic security tools. You don’t even realize that you are about to master the very basic principles of Python coding.it is undoubtedly one of the best resources to combine IT security pen testing and hacking with Python scripting.  
 [**Black Hat Python-Python Programming for Hackers and Pen-testers :**](http://www.amazon.in/gp/product/1593275900/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=1593275900&linkCode=as2&tag=proethhacsway-21&linkId=3UUBAHT5H5J66CR5)Black Hat Python explores the darker side of Python's capabilities writing network sniffers, manipulating packets, infecting virtual machines, creating stealthy Trojans, extending the popular web hacking tool Burp Suite, and more.If you're penetrating a network, this book is for you.  
  
**Reverse engineering :**  
  
[**Reversing - Secrets of Reverse Engineering:**](http://www.amazon.in/gp/product/0764574817/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=0764574817&linkCode=as2&tag=proethhacsway-21&linkId=GQAK7JFD45FQAGHB) The author walked you through the techniques which can be used in reverse/anti-reverse software. Most of them can be applied and used when you do your own code reverse. The book also teaches you how to protect your own application from reversing.  
  
  
[**The.IDA.Pro.Book.2nd.Edition:**](http://www.amazon.in/gp/product/B004OEJNTM/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=B004OEJNTM&linkCode=as2&tag=proethhacsway-21&linkId=D73GPZ6C5SGVGQSW)IDA Pro is a very powerful tool that is very difficult to learn and use this is a book on how to use IDA, not a book on how to read dis-assembly.If you want to learn to use IDA Pro, this is by far the best book for you.  
  
[**Gray Hat Python-  Python Programming for Hackers and Reverse Engineers:**](http://www.amazon.in/gp/product/1593271921/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=1593271921&linkCode=as2&tag=proethhacsway-21&linkId=C46XK3CXGF6GYKFL)  Gray Hat Python explains the concepts behind hacking tools and techniques like debuggers, trojans, fuzzers, and emulators. If you use python for your day-to-day scripting  and perform some reverse engineering/debugging/fuzzing tasks, then this definitely a book that is bound to catch your attention.  
  
[**Hacker Disassembling Uncovered-Powerful Techniques To Safeguard Your Programming:**](http://www.amazon.in/gp/product/1931769222/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=1931769222&linkCode=as2&tag=proethhacsway-21&linkId=IMS5TKF4ILHLNVGR)It's a good primer to the art of reverse engineering. if you are a system and/or kernel mode programmer, then this is the book for you. This book deals with how to go about disassembling a program with holes without its source code.  
  
[**Programming from the ground up** :](http://www.amazon.in/gp/product/0975283847/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=0975283847&linkCode=as2&tag=proethhacsway-21&linkId=D4MCFH3463JGHCKZ) Programming from the Ground Up uses Linux assembly language to teach new programmers the most important concepts in programming. It takes you a step at a time through assembly language concepts.The examples are very simple and the language used throughout the book is very easy to understand.  
  
**Shellcoding and exploit development :**  
[**A Bug Hunter's Diary - A Guided Tour Through The Wilds of Software Security :**](http://www.amazon.in/gp/product/B00652XO2I/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=B00652XO2I&linkCode=as2&tag=proethhacsway-21&linkId=IASTEIWURJOTYAEC)This book gives valuable insights on different techniques of bug hunting and exploiting them successfully. Each of the chapters in this book conforms to the each of the vulnerability discovered by author and written in his own words and style. The author exploits bugs in some of the world's most popular software, like Apple's iOS, the VLC media player, web browsers, and even the Mac OS X kernel.  
  
[**Sockets, Shellcode, Porting & Coding - Reverse Engineering Exploits And Tool Coding For Security Professional:**](http://www.amazon.in/gp/product/B007MLVDME/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=B007MLVDME&linkCode=as2&tag=proethhacsway-21&linkId=NHAOU6EF7VMLC74D)When I saw this book I thought I had found what I was looking for.I personally like this book.The book is logically divided into 5 main categories(coding, socket,porting, shellocode,coding tools) with each category representing a major skill set required by most security professionals. But remember you have a knowledge of reverse engineering.  
  
[**The.Shellcoders.Handbook.2nd.Edition:**](http://www.amazon.in/gp/product/047008023X/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=047008023X&linkCode=as2&tag=proethhacsway-21&linkId=H3KB6B4G3TDEWUXZ) This is a very good book on software vulnerabilities. this book is about code and data and what happens when the two become confused. You'll work with the basic building blocks of security bugs—assembler, source code, the stack, the heap, and so on. You'll experiment, explore, and understand the systems you're running—and how to better protect them.  
  
[**Exploiting Software- How to Break Code:**](http://www.amazon.in/gp/product/B0072HYX2A/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=B0072HYX2A&linkCode=as2&tag=proethhacsway-21&linkId=JWAQQAAIGY3UOR4R)This book describes basic attacks on application software.it uses the pedagogical device of teaching how software can be attacked to achieve the goal of explaining how secure software should be built.it is a very exciting book, full of nitty-gritty details you need to be familiar with in order to understand how attackers find software holes and build exploits. These details are really valuable if you want a deep understanding of the concepts and practices behind system security.  
  
[**Buffer Overflow Attacks -  Detect, Exploit, Prevent:**](http://www.amazon.in/gp/product/1932266674/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=1932266674&linkCode=as2&tag=proethhacsway-21&linkId=VVOALHWIGXLFL5JL) This book clearly explains the basics of stack overflow, off by one, heap overflow and string format attacks. You do need some familiarity with assembly.This gives step by step examples in reading, creating and disassembling shellcode and buffer overflows. if you want to write buffer overflow attack code from grounds up, spanning from Linux, freeBSD to Windows, this book is for you.  
  
**Web-Hacking :**  
[**The.Web.Application.Hackers.Handbook:**](http://www.amazon.in/gp/product/B005LVQA9S/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=B005LVQA9S&linkCode=as2&tag=proethhacsway-21&linkId=RM6RNATQXUDGN55B) This is by far the best book I've ever read on web application security. If you do any type of professional Web Application Assessments then this is your bible.This book is a practical guide to discovering and exploiting security flaws in web  applications.  It allows the reader to step into the shoes of hackers and see the world through their eyes.  
  
[**Botnets The Killer Web Applications Hacking**:](http://www.amazon.in/gp/product/B00RLXT6PO/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=3626&creative=24790&creativeASIN=B00RLXT6PO&linkCode=as2&tag=proethhacsway-21&linkId=AEFOXI5ICURDKVQA) This is the first book to explain the newest internet threat Botnets, zombie armies, bot herders, what is being done, and what you can do to protect your enterprise.this is a must for those of us that wants to understand the underground aspects of botnet. Botnets are the most complicated and difficult threat the hacker world has unleashed - read how to protect yourself.  
  
**8. Important Toolkit for Ethical Hackers and  Penetration testers:**  
  
[**Kali-linux** :](https://www.kali.org/)Kali Linux is an advanced Penetration Testing and Security Auditing Linux distribution.It has more than 300 penetration testing tools.  
  
[**Metasploit:**](http://www.metasploit.com/)This is the most advanced and popular Framework that can be used to for pen-testing. It is based on the concept of ‘exploit’ which is a code that can surpass the security measures and enter a certain system.  
  
[**Namp:**](http://nmap.org/)This is a very popular tool that predominantly aids in understanding the characteristics of any target network. The characteristics can include: host, services, OS, packet filters/firewalls etc.  It works on most of the environments and is open sourced.  
  
[**Wireshark :**](https://www.wireshark.org/)Wire-shark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. Penetration test tools like Wireshark come in handy for understanding and exploiting the data organization posted by forms or services to applications. Application vulnerabilities such as parameter pollution, SQL injection, lack of input validation, as well as buffer overflow can be easily detected and exploited using Wireshark.  
  
[**Nessus**](http://www.tenable.com/products/nessus)**:** Nessus is a great tool designed to automate the testing and discovery of known security problems. Typically someone, a hacker group, a security company, or a researcher discovers a specific way to violate the security of a software product.  
  
[**Cain & Abel :**](http://www.oxid.it/cain.html) Cain and abel is one of best Tool that is commonly used to Poison the network If cracking encrypted passwords or network keys is what you need, then Cain& Abel is the tool for you. It uses network sniffing, Dictionary, Brute-Force and Cryptanalysis attacks, cache uncovering and routing protocol analysis methods to achieve this.  
  
[**John The Ripper :**](http://www.openwall.com/john/)This is the most powerful  password cracker tool. This tool works on most of the environments, although it’s primarily for UNIX systems. It is considered one of the fastest tools in this genre. Password hash code and strength-checking code are also made available to be integrated to your own software/code.  
  
[**OWASP Mantra**](http://www.getmantra.com/)**:** Mantra is a browser especially designed for web application security testing.Mantra has many built in tools to modify headers, manipulate input strings, replay GET/POST requests, edit cookies, quickly switch between multiple proxies, control forced redirects etc. This makes it a good software for performing basic security checks and sometimes, exploitation. Thus, Mantra can be used to solve basic levels of various web based CTFs, showcase security issues in vulnerable web applications etc.   
  
[**Acunetix:**](http://www.acunetix.com/vulnerability-scanner/) Acunetix is essentially a web vulnerability scanner targeted at web applications. It provides SQL injection, cross site scripting testing, PCI compliance reports etc. along with identifying a multitude of vulnerabilities.  
  
[**Burp Suite :**](http://portswigger.net/burp/)This tool is used to performing a Web Application Penetration Test. Burp Suite contains all the Burp interfaces and tools made for speeding up and facilitating the process of application attacks.   
  
[**Havij pro**](http://www.itsecteam.com/products/havij-advanced-sql-injection/) : Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page. It can take advantage of a vulnerable web application. By using this software, user can perform back-end database fingerprinting, retrieve DBMS login names and password hashes, dump tables and columns, fetch data from the database, execute SQL statements against the server, and even access the underlying file system and execute operating system shell commands.