# Complete guide to become an Ethical Hacker

http://programmingethicalhackerway.blogspot.in/

# Professional Ethical Hacking course

- CEH(certified ethical hacker):The Certified Ethical Hacker is a professional certification, provided by the EC-Council.
- SANS Security : SANS is by far the largest source for information security training and security certification in the world.
- Offensive security: Offensive security offer many types of information security certification courses like OSCP(offensive security certified professional),OSEE...

http://programmingethicalhackerway.blogspot.in/

# Resources : Books

- Google might not help for Proper resources of learning hacking.
- Here i will share my experience
- So let’s start…….

http://programmingethicalhackerway.blogspot.in/

# Books: for learning hacking

- **Hacking: The Art of Exploitation** : very good book on the subject of hacking.
- **The Hacker's Underground Handbook** :If you are coming from a position of absolutely no knowledge of the hacking, this may be useful to you.
- **Gray Hat Hacking -The Ethical Hackers Handbook**
- **Violent python -A Cookbook for Hackers** :great for those who are new to the python language and would like example use cases of simplistic security tools
- **Black Hat Python-Python Programming for Hackers and Pentesters** :explores the darker side of Python's capabilities writing network sniffers, manipulating packets, infecting virtual machines, creating stealthy Trojans.

# Books: for Reverse Engineer

- **Reversing - Secrets of Reverse Engineering**: walked you through the techniques which can be used in reverse/anti-reverse software.
- **The.IDA.Pro.Book.2nd.Edition** : this is a book on how to use IDA, not a book on how to read dis-assembly.
- **Gray Hat Python- Python Programming for Hackers and Reverse Engineers**
- **Hacker Disassembling Uncovered-Powerful Techniques To Safeguard Your Programming** : a good primer to the art of reverse engineering and deals with how to go about disassembling a program with holes without its source code
- **Programming from the ground up** : takes you a step at a time through assembly language concepts

# Books: for Shellcoding and exploit

- **A Bug Hunter's Diary** : gives valuable insights on different techniques of bug hunting and exploiting them successfully
- **Sockets, Shellcode, Porting & Coding** : divided into 5 main categories with each category representing a major skill set required by most security professionals.
- **The.Shellcoders.Handbook.2nd.Edition** : This is a very good book on software vulnerabilities.
- **Exploiting Software- How to Break Code** : describes basic attacks on application software.
- **Buffer Overflow Attacks - Detect, Exploit, Prevent** : This book clearly explains the basics of stack overflow, off by one, heap overflow and string format attacks.

http://programmingethicalhackerway.blogspot.in/

# Books:  for Web-Hacking

- The.Web.Application.Hackers.Handbook :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.

- Botnets The Killer Web Applications Hacking :This is the first book to explain the newest internet threat Botnets, zombie armies, bot herders.

- OWASP :The Open Web Application Security Project is an online community dedicated to web application security.

# Important Toolkit for Hackers

- **Kali-linux** : Kali Linux is an advanced Penetration Testing and Security Auditing Linux distribution.It has more than 300 penetration testing tools.
- **Metasploit** : most advanced and popular Framework that can be used to for pen-testing.
- **Namp** : very popular tool that predominantly aids in understanding the characteristics of any target network.
- **Wireshark** : Wireshark 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
- **Nessus** : Nessus is a great tool designed to automate the testing and discovery of known security problems.

# .....Continue

- **Cain & Abel** :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.
- **John The Ripper** : This is the most powerful password cracker tool.
- **Acunetix** : Acunetix is essentially a web vulnerability scanner targeted at web applications. It provides SQL injection, cross site scripting testing, PCI compliance reports etc.
- **Burp Suite** : This tool is used to performing a Web Application Penetration Test.
- **Havij pro** : Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.

# Final words….

- Here I share my whole experience with you.Hope this guide will help you.
- In your hacking journey, you will face many challenges. Always one thing keep in mind ”Don’t give up”
- Sometime frustration stage comes where you need “Be patient”
- Always “Face challenges smartly”
- You Won’t become an hacker overnight; it takes years of practice and real world experience to become professional hacker.

http://programmingethicalhackerway.blogspot.in/

# Contact ME:

- Follow Me on Google+ : SANDEEP SAINI
- Visit My Blog : **Programming:Ethical Hacker Way**
- Like blog on facebook :Programming:Ethical Hacker Way

http://programmingethicalhackerway.blogspot.in/

# Who is ethical hacker?

- A hacker is someone who exploit the vulnerability in system.
- A ethical hacker is someone who exploit the vulnerability in system with permission of owner.
- The ethical hackers may also known as grey hat or white hat hackers .

# The end

**Let’s start your hacker journey and enjoy it……..**

**Best Wishes**

http://programmingethicalhackerway.blogspot.in/

# may I become a hacker ?

- YES.. Everyone can become a hacker.
- Always think like a hacker.
- A hacker thinks how it works, what if it is not so, what if i do so, It works in my control
- A hacker is curious to learn, keep patience,deeply aspiring to learn.
- In simple words, with zero technical knowledge everyone can become a hacker.

http://programmingethicalhackerway.blogspot.in/

# What needs to learn to hacker?

- Learn about computer system
  - hacker should have good knowledge about operating systems(Unix and Windows)
- Learn Programming
  - computer hacker : C/C++,Python,Assembly
  - web hacker : HTML, Javascript, PHP, SQL
- Learn Networking.
- Join Hacker Forums.

http://programmingethicalhackerway.blogspot.in/

# Resources to learn

- Programming
  - C programming in hacker way
  - Assembly programming in hacker way
  - Python programming in hacker way
- Networking for hackers
- Join hackers forums on social websites like Facebook, Twitter.
- Some facebook groups recommend :
  - Programming : Hacker's Way
  - H4cK!nG: F0r B3g!nn3r
  - Security Researchers
- join ethical hacking communities like HackThisSite, Black-Hat Forums etc.

http://programmingethicalhackerway.blogspot.in/

# Hacker Profession

- As a doctor have a special profession like  Dentist, Allergist, Surgeon... the hacker have also a special profession.
- The hackers profession are exploit writer, vulnerability researcher, security researcher, shellcode writer, reverse engineer, virus and malware writer, penetration tester, network hacker, web-application hacker, computer hacker and many more….
- a simple mean of hacker is penetration tester who enters the system.

## Which hacker profession should elect ?

- i would recommend “Choose According to Your Passion”.

# Hackers profession in detail

- A computer hacker is someone who hack machine or computer
- A exploit writer is someone who exploit the vulnerability of  a program
- A shellcoder is someone who writes shellcodes that can be injected in an application and returns a remote (or local) shell when executed
- A security researcher is someone who finds the security hole in the system and makes it secure.

# …..Continue

- A reverse engineer is someone who breaks the compiled code for ethical or unethical purpose.
- A virus and malware writer is someone who writes the malicious code with malicious intentions.
- A web-application hacker is someone who hack websites or find web-application vulnerabilities.
- A network hacker is someone who hack network like sniffing, pack-crafting, breaking IDS rules or firewall, packet capturing and more…
- I think now you must have an idea about your passion.

http://programmingethicalhackerway.blogspot.in/