

## **Expert Hacker - XW (EHXW)**

### **Training Syllabus**

IL Hack Institute: Expert Hacker – Exploit Writer (EHXW)  
5 Days Training.

Day 1:

- Introduction to exploit writing
  - Operating Systems differences
  - Windows for Exploit writing
  - Linux for Exploit writing
  - Setting up an Exploit writing lab
- Programming Intro
  - The ASM language
  - Intel ASM syntax
  - AT&T ASM syntax
  - C language for XW
  - Script languages
  - Python script language for XW

## Day 2:

- Exploits in the wild
  - How to find exploits on the internet
- Shellcode
  - How to write shellcodes
  - How to find shellcodes
- Overflows
  - What are overflows
  - Buffer overflows
  - Stack overflows in windows
  - Stack overflows in linux
- Debuggers
  - Windows debuggers
  - Linux debuggers

## Day 3:

- Overflows
  - Heap overflows in windows
  - Heap overflows in linux
  - Format string attacks
- Fuzzing
  - Manual and automated fuzzing
  - Fault Injection
  - How to build a fuzzer

## Day 4:

- Reverse engineering
  - Using IDA
  - Reversing a windows application
  - .Net applications
  - Anti debuggers
  - Software cracking

## Day 5:

- Writing real world exploits
  - Writing a real buffer overflow exploit
  - Writing a real heap overflow exploit
  - Writing a real format string exploit
- Conclusive lab