

## **Expert Hacker - PT (EHPT)**

### **Training Syllabus**

IL Hack Institute: Expert Hacker – Penetration Tester (EHPT)  
5 Days Training.

Day 1:

- Introduction to Hacking
  - Introduction to Penetration Testing
  - Operating Systems
  - Windows for PT
  - Linux for PT
  - Setting up a PT lab
  - TCP/IP
  - Building an attack tree
- Information gathering
  - Passive information gathering
  - Active information gathering
  - Google Hacking

## Day 2:

- Enumeration
  - Port scanning
  - Services enumeration
  - OS enumeration
  - Web enumeration
  - SNMP enumeration
- Scanning, Spoofing and Sniffing
  - Nmap and others
  - Cain & Able and others
  - WireShark and others
  - Traffic analysis

## Day 3:

- Penetration
  - Infrastructure PT
  - Metasploit Framework
  - Password Cracking
  - DoS/DDoS
  - Privilege escalation

## Day 4:

- Penetration
  - Application PT
  - Data interception and Proxies
  - Client Side attacks
  - Injection Attacks
  - Cross Site Scripting (XSS)
  - CSRF
  - Data manipulation attacks

## Day 5:

- The CISO Position
  - How to write PT reports
  - Managing information security
  - Information security regulations
- Conclusive lab