



Ethical Hacking Course

# HANDS-ON HACKING UNLIMITED

There are many ways to counter today's security problems. Knowing the hacking mindset is the most important of these. How, in other words, a hacker thinks, behaves and acts - what techniques and methodologies are used by the hacker to take advantage of current existing vulnerabilities.

With this in mind, Hands-on Hacking Unlimited has been created for IT professionals, security officers, network administrators and others who wish to understand what really happens whenever an attack is perpetrated and which vulnerabilities are exploited by hackers.

Hands-on Hacking Unlimited offers an effective and complete perspective with a focus on network vulnerabilities and an in-depth analysis of the most critical vulnerabilities, targets and concerns.

## Training Overview

This course is targeted at IT professionals who wish to learn the various hacking and defensive techniques used by hackers to compromise an organization's IT infrastructure. The course offers a set of live simulations and live labs featuring a variety of missions on proprietary targets.

## Who Should Attend?

- IT managers
- IT security specialists
- Security officers
- Network administrators
- Individuals and enthusiasts interested in this topic

## Course Contents

This intensive, two-day seminar touches on many areas of IT security. Below is the complete program:

### General introduction to ethical hacking

What is ethical hacking  
Legal involvements

### Target information acquisition

Passive and active footprinting via  
Whois, Dig, Traceroute, Google  
[Live session](#)

### Nmap

Advanced utilization of the most famous network scanning tool  
Port scanning  
Host discovery  
Web/DB/Mail auditing  
Nmap scripting engine  
[Live session](#)

### Vulnerability identification

Detailed analysis on the techniques used to obtain an accurate network mapping  
Network mapping  
Nmap, Nessus, OpenVAS and others  
Google dorks  
[Live session](#)

### Cover your tracks

Proxy  
DNS tunneling  
SSH tunneling  
ICMP tunneling  
Tor  
VPN

### Different kinds of exploits

Where to find them  
Which to choose  
How to use them  
How to write them  
[Live session](#)

### Metasploit

Advanced utilization of the framework that turned the hacking world upside down  
[Live session](#)

### Password cracking

Retrieve password hashes on Windows and \*nix OSes  
Ophcrack, Hashcat  
Rainbow tables  
Brute force with Cuda  
Hydra  
[Live session](#)

### Tapping secure communications through Heartbleed

[Live session](#)

### Botnet

What they are  
Build your own botnet

### VOIP hacking

How to exploit VOIP weaknesses  
Enumeration  
Eavesdropping  
VLAN hopping  
[Live session](#)

### VNC hacking

Authentication bypass  
VNC password cracking

### X11 hacking

Exploiting X servers misconfigurations  
Xdotool  
Xwd  
[Live session](#)

### IPMI hacking

Common vulnerabilities against various BMC brands  
Ipmitool  
Cipher zero  
Hash retrieval

### Man in the Middle attacks

Common protocols analysis  
Communication packets analysis  
MitM attack techniques  
Wireshark, Ettercap and others  
[Live session](#)

### Social engineering

Introduction to Phishing and other social engineering techniques  
BEEF, SET and others

### Web attacks

Introduction to the mostly used attacks against web applications SQLMap, Burp suite e altri

## What You Will Learn

How to think like a hacker to improve protection of your system.  
How to discover and exploit discovered vulnerabilities. Typical techniques used to gain access into a system.

## Course Style: Live Hacking!

### Duration

2 days

### Prerequisites

Background in Microsoft Windows and Linux is desirable. Knowledge of TCP/IP protocols.

### About Zone-H

Zone-H is an independent and open-source digital observatory, considered today as the most authoritative voice on cybercrime of the Internet. The [www.zone-h.org](http://www.zone-h.org) homepage registers about 35.000 single accesses, for a total of nearly 800.000 clicks, on an average day.

Supported by a worldwide community of more than 50 experts, among which are IT professionals, journalists, students and scholars, Zone-H present a realistic and "no-hat" perspective on web trends.

Information and analysis on cyber terrorism and cybercrime, IT Security services and educational programs are available to the IT community, that every day can count on our advisories, statistics, updates and news, coming from constant web monitoring activities. The data produced merge into one of the biggest digital archive in the world, including to date, over 11,000,000 recorded attacks and providing information on the attackers profiles, motivations and methodologies of intrusion.

Worldwide educational programs focusing on the fundamental aspects of IT Security address a variegated and international public, promoting "ethical hacking" techniques from a unique source of comprehensive information and hacker intelligence.



[www.zone-h.org](http://www.zone-h.org)