



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 Hacking

#### Collecting Information on our Target

Web-based instruments: Google, Netcraft, Visualroute, etc.

Local instruments: scanners, fingerprinters, etc.

#### Extended Network Mapping

A detailed analysis of the techniques to be used for executing network mapping:

Passive and active resources, DNS bruteforcing, Zone Transfer.

Live session

#### Collecting Information on Old and New Vulnerabilities

#### Protecting Anonymity while Hacking (shells, proxys, tor)

#### Live Session on Gathering Information on Various Targets

#### The Typical Structure of a Web Site

Enumeration of the components and their inherent possible vulnerable points.

#### Vulnerabilities

Encrypted communication lines, Firewalls and routers, Webservers (Apache/IIS), Applications, Databases.

#### What is an Exploit?

#### Introducing and Exploiting Most Common Linux Vulnerabilities

SSH, SSL, Apache, Others.

Live session

#### Introducing and Exploiting Most Common Windows Vulnerabilities

Frontpage extension, The ever-present Unicode, Others.

Live session

#### Buffer Overflows: after decades, still one of the most severe vulnerabilities

Local Buffer Overflow, Remote Buffer Overflow.

Live session

#### Man in the Middle: a particular category of attacks

ARP Poisoning, DNS Poisoning, ICMP Redirect.

#### Passwords

Password Security, Hacking Instruments.

#### Exploiting Database Vulnerabilities

SQL Injection, URL Poisoning.

Live session

#### Cross Site Scripting

Learn how a technique, considered by some as banal, allows in fact attackers to obtain surprising results:

Site hijacking, Session hijacking, Reprogramming network components, HTML principles and vulnerabilities. Online session against banking, open forum, e-mail sessions.

#### Black Box Hacking Session

Hacking an unknown Windows system.

Hacking an unknown Linux system.

Hacking an unknown OS system.

Live session

#### Social Engineering: techniques and psychological traps

#### Attacks Against the User: malware

#### 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. Zone-H websites are available in 13 different editions: English, Italian, French, Russian, Brazilian, Slovak, Spanish, Japanese, Slovenian, Turkish, German, Latvian and Croatian.

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 2,000,000 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.