Ethical Hacking Course

HANDS-ON HACKING UNLIMITED

There are many ways to counter today's security problems. Sure enough, knowing the hacking mindset, how in other words a hacker think, behaves and what techniques and methodologies are used to take advantage of current existing vulnerabilities is the most appropriate one.
With this is mind, *Hands-on Hacking Unlimited* has been created for IT professionals, security officers, network administrators who wishes to understand what really happens whenever an attack is perpetrated and which vulnerabilities are exploited.

Hands-on Hacking Unlimited offers an effective and complete perspective on logical security issues through a lateral-thinking approach to system security, combining ethical hacking fundamentals with an in-depth analysis of the most critical areas.

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 is designed both for those who have already acquired hacking and security basics and for those who are approaching the subject for the first time, and wishing to acquire a comprehensive background and solid practical skills.

Who Should Attend?

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

zone-h
the internet thermometer

HANDS-ON HACKING UNLIMITED

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 Extended Network Mapping:
- Passive and Active Resources
- DNS brute-forcing
- Zone Transfer

Live session

Collecting information on old and new vulnerabilities

Protecting anonymity while hacking (theory about shells and proxies)

Rootkits

Trojans

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

Cross-site scripting

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

Internet Explorer
The most devastating vulnerabilities in Internet Explorer. How to gain control of a PC through IE vulnerabilities. Examples on how to use three different vulnerabilities for executing an arbitrary code on a PC are showcased.
Live session

Exploiting database vulnerabilities:
- SQL injection
- URL poisoning

Live session

Black box hacking session:
- Hacking an unknown Windows system
- Hacking an unknown Linux system
- Hacking an unknown OS system

Live session

The theory behind Buffer Overflows

How to properly follow-up the system patching

Social engineering: techniques and psychological traps

Future hacking playgrounds:
Home automation systems, 3rd generation mobile phone platforms

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
- How to conceal tracks
- How to collect information and profile information systems
- How to find and use hacker toolboxes

Course Style: Live Hacking!

The course is lector-led, using hacking simulations to illustrate potential threats. Numerous practical case studies will be provided as working examples.

Duration

2 days

Prerequisites

Background in Microsoft Windows and Linux is required. Basic programming skills are also desirable.

About zone-h

Uniquely positioned as the Internet most authentic source on web attacks and cybercrimes as an independent observatory, zone-h each day chronicles cyber attacks, network breaches and web site defacements as reported by both sides, attackers and defenders.
With a no-hat approach zone-h gives proper and punctual coverage on what's going on the Net every single day of the year with news, advisories, opinions, statistics, forums and, most important of all, with the most authoritative and complete server-side cybercrime database available today.

zone-h
the internet thermometer

www.zone-h.org www.zone-h.it www.fr.zone-h.org www.ru.zone-h.org