



# Ethical Hacking Training

<http://www.scanit.net/courses/ethical/>

## Overview

During the 5 day course, you will be working with engineers who work exclusively in the fields of penetration testing and ethical hacking. Being guided through theoretical and practical exercises to hone you instincts, and open your eyes to the ways in which people attack your infrastructures.

## Course Pre-requisites

Students should have reasonable understanding of:

- TCP/IP
- Unix
- Windows 2000/2003

## Course Materials

- CD with tools used during labs
- English Course Notes
- Scripts
- Hacking Exposed Book

## Course Duration

5 days

## Table of Contents

### Information Gathering

- Using publicly available information to target the attack
- Internet Relay Chat - IRC
- Social engineering
- Using DNS information for hacking
- Port scanning
- Operating system fingerprinting
- Banner grabbing
- War dialing
- War driving – wireless networks

### Windows Hacking

- Windows security architecture
- Windows networking
- Windows - specific information gathering
- Remote attacks
- Local privilege escalation

### Unix Hacking

- Unix security architecture
- Unix - specific information gathering
- Programming errors resulting in security vulnerabilities
- Buffer overflows, Race Conditions
- Incorrect input validations

### Web Hacking

- Getting information from the web-server
- Classification of web vulnerabilities (buffer overflows, directory traversal, incorrect input validation, encoding/decoding bugs, etc.)
- Scanning for known vulnerabilities
- Checking for configuration errors
- Escalating privileges
- Assessing the security of custom Web Applications

### Miscellaneous topics

- Checking known vulnerabilities
- Router configuration errors
- Password cracking
- Firewalls
- Intrusion Prevention Systems
- Use and misuse of encryption for security purposes
- Rootkits and trojans
- E-mail Hacking

**Hacking contest -**  
**on the last day of the course**