

Rui Pereira, B.Sc.(Hons), CIPS ISP, CISSP, CISA, CWNA, CPTS/CPTE  
Principal Consultant, WaveFront Consulting Group  
[ruiper@wavefrontcg.com](mailto:ruiper@wavefrontcg.com) | 1 (604) 961-0701 | [www.wavefrontcg.com](http://www.wavefrontcg.com)

*"If you know the enemy and know yourself, you need not fear the result of a hundred battles."*

Sun Tzu on "The Art of War"

Hardly a day goes by without news of yet another computer security incident - Viruses, worms, Trojans, spyware; Identity theft; Stolen credit card numbers; Denial of Service attacks; Disclosure of private information; Website defacement; Phishing and Pharming attacks; Botnets and Zombies; etc. Organizations and individuals are continually being advised to take security precautions against this constant stream of attacks - Firewalls, VPN's, Anti-virus software, patching, practicing safe e-mail and surfing habits, encrypting data, carrying out vulnerability assessments, etc. Yet, despite all these precautions, the attacks continue unabated, and cyber-crime remains a plague on the Internet, causing millions of dollars of losses each year.

But how do cyber-criminals and hackers attack our systems and networks? How is it possible for an attacker to take over (or "own", in hacker parlance), another computer? An attacker has to find only one weakness in order to break into a system or network. Systems, network and security professionals have to defend against every possible form of attack. This asymmetry between attack and defense means defenders are at a distinct disadvantage. *Knowing the enemy and their techniques* can help to even out that imbalance - it can be extremely useful to better allow defenders to protect the systems and networks under their control.

## **Course Description**

This four-day course is based on Sun Tzu's principle that knowing one's enemy will strengthen one's defenses and more adequately prepare one for battle. It is better for us to find the vulnerabilities in our own systems ourselves and fix them, before the hackers and cyber-criminals find the same vulnerabilities and exploit them for fun and profit. Penetration testing allows us to simulate hacker attacks, and so test our own defenses to verify they are adequate.

This course describes the major hacking techniques, shows how to determine one's own vulnerability to such attacks, and how to protect against them. Students will work through hands-on exercises (labs) where they will attack vulnerable test systems, fix the vulnerability that was exploited, and then attempt to attack the system again to verify that the protection mechanisms are working correctly. With this enhanced understanding of hacking techniques, students will be in a better position to appreciate the hacker threat, and better equipped to defend their organizations against hacking attacks.

## **Our Trainer**

This course was developed and is presented by our Chief Trainer, Mr. Rui Pereira, B.Sc.(Hons), CIPS ISP, CISSP, CISA, CWNA, CPTS/CPTE. Rui is a Certified Penetration Testing Specialist (CPTS) and Certified Penetration Testing Expert (CPTE). He has over 25 years of experience in the IT industry, the last 13 in Information Security and Audit (with many penetration tests and vulnerability assessments under his belt). In addition to WaveFront's suite of IT Security courses, Rui has also developed and teaches several courses at the University of British Columbia (UBC) and the British Columbia Institute of Technology (BCIT). Rui's biography and resume are available online at <http://www.wavefrontcg.com/PrincipalConsultants.html>.

## Pre-Requisites

The course is intended for security professionals, auditors, and system and network administrators. A good technical understanding of computer systems (primarily MS Windows) and networks (TCP/IP) is a pre-requisite for taking this course. UNIX/Linux experience is not necessary. However, since many hacking tools are Linux based, students will be given some background training on this environment. All necessary equipment and software will be provided.

## Learning Outcomes

At the end of this course the student should be able to:

- Understand the hacker threat and the major techniques used by hackers;
- Understand the need for penetration tests and vulnerability assessments, and be able to initiate and manage these assessments;
- Understand the moral, ethical and legal considerations of penetration testing and ethical hacking;
- Use various hacking and vulnerability assessment tools to assess the security of their own networks and systems;
- Locate vulnerability, exploit and fix information on the Internet;
- Identify and fix vulnerabilities and mis-configurations in major computer technologies;

## Course Outline

### Day 1 - **Introduction to Penetration testing**

Course Overview and Approach

The Threat Landscape

The Vulnerability / Exploit Life-Cycle

The Law

US and Canadian Legislation, PCI DSS

Hacking and InfoSec Background

Terminology, Vulnerabilities and Exploits

Security Assessments

Penetration Tests, Other Types of Security Assessment

Ethical, Legal and Contractual Requirements

Code of Ethics

Further Training and Certifications

### **Pen-testing / Ethical Hacking Methodology**

Methodology

A 12-step Process, Skills for Pen-Testers

Attack Types Overview

Hacking Tools Overview

Methodology in Action [Demo]

Attacking a Windows Web Server

Pivoting the Attack

Attack Countermeasures

## **Defences**

Corporate and Personal Defences  
Protecting Yourself (as a pen-tester)

## **The Lab Environment**

Your Workstation  
VMWare and Virtual Machines

## **Cryptography for Pen-Testers**

Conceptual Foundation  
Building Blocks

- Symmetric and Asymmetric Cryptography
- Message Digests
- Public Key Infrastructure (PKI)
- Hybrid Crypto-Systems

Cryptography for Network Traffic

- SSL, IPSec, PGP

Cryptography for Data at Rest

- File and Database Encryption, Password Storage

Key Management  
Attacking Crypto

- Cryptographic and non-Cryptographic Attacks

Day 2 -

## **Hacking Tools and Techniques**

Information Gathering (Recon)

- Network Utilities and Websites
- Google Hacking
- Information Gathering Tools (Nikto, Wikto, Maltego)

Port Scanning

- NMap, Other Port Scanners (SuperScan, Look@Lan, etc.)

Vulnerability Scanning

- Nessus, Other Vulnerability Scanners (SAINT, XScan, etc.)

Exploits

- Buffer Overflows, Format String Vulnerabilities
- Other Exploit Types (Race Conditions, Integer Overflows, etc.)
- Finding and Using Exploits (SecurityFocus, Milw0rm)

Exploit Frameworks

- Metasploit
- Other Exploit Frameworks (Core Impact, SAINT Exploit, etc.)

Live Linux CD's

- BackTrack, Other Live Linux CD's

- Password Cracking
  - Online Cracking (Hydra)
  - Dictionary and Brute Force Attacks
  - Rainbow Tables (OphCrack)
  - Windows, UNIX, Oracle and Other Password Systems
  - Password Cracking Tools (John the Ripper, Cain&Abel)

Day 3 - **Hacking Tools and Techniques (continued)**

- Using Malware
- Denial of Service Attacks
- Sundry and Useful (Netcat, VNC, tftp, etc.)

**Network Attacks**

- Firewalls
- Routers and Switches
- IDS/IPS
- Network Sniffing
  - Active vs. Passive Sniffing, Wireshark
- Man-in-the-Middle Attacks
  - ARP Spoofing
  - DNS Cache Poisoning
  - Breaking SSL
  - MITM Tools (Cain&Abel, Ettercap)

**Breaking Windows**

- Password Weaknesses
- Null Sessions
- Active Directory
- Local and Remote Exploits
- Covering Your Tracks

**Hacking UNIX/Linux**

- Linux Background
- Exploiting Services
- Symbolic Links and SUID Files
- Local and Remote Exploits

**Hacking Web Servers**

- General Attacks
- Hacking Apache
- Hacking IIS
  - Directory Traversal Attacks
- Web Application Security\*

Day 4 - **Hacking Databases**

Database Background  
Indirect Database Attacks  
    SQL Injection\*  
Direct Database Attacks  
    Stealing Passwords  
    Scanning Tools (Scuba)  
Hacking Oracle  
Hacking Microsoft SQL Server

**Hacking Wireless**

Tools and Techniques\*

**Hacking VoIP**

Phreaking and War-Dialing  
VoIP Attacks

**Penetration Testing Exercises**

Students use the techniques learned during the course to attempt to break into a (somewhat) vulnerable server. This can be done individually or in groups, and guidance is provided by the instructor.

Contact Rui Pereira at [ruiper@wavefrontcg.com](mailto:ruiper@wavefrontcg.com) or 1 (604) 961-0701 to book a place on the next presentation, or for further information. This document is also available online at [http://www.wavefrontcg.com/Hacking101\\_2009a.pdf](http://www.wavefrontcg.com/Hacking101_2009a.pdf).

\* A more in-depth treatment of these topics is provided in our companion courses "[Secure Web Application Development and Testing](#)" and "[Wireless Network Security Complete](#)" (under development).