

# Free Penetration Testing Workshop in Bristol, UK

**Source:**

<http://www.tech-archive.net/Archive/Certification/microsoft.public.cert.exam.mcse/2004-10/1379.html>

---

**From:** ExecuTrain (*ExecuTrain\_at\_discussions.microsoft.com*)

**Date:** 10/21/04

Date: Thu, 21 Oct 2004 04:19:03 -0700

This three-hour Penetration Testing workshop will introduce attendees to hacking techniques and methods used to break into networks. Attendees will learn how the focus of security has changed in recent years and will see how penetration testing can make a huge difference in your security program. Attendees will see live or simulated demonstrations of attacks on computer systems. There will also be a Metasploit demonstration with directions and the tools given to attendees to practice at home. Seeing the ease with which these attacks are carried out will demonstrate the problems faced by information security personnel every day.

Knowing how attacks are carried out is the first step to defending against them. Penetration Testers provide an invaluable service to those defending networks worldwide. This seminar is not a sales event—it is a presentation by an experienced security professional with years of network attack and defense experience. Attendees will LEARN about penetration testing and hacking. They will not just see a demonstration of the frightening tools and attacks.

**Outline:**

1. Who are the Hackers?
  - o Introduction
  - o Attackers; Hackers; Crackers
  - o How do they work?
  - o Statistics
2. Hacker's Methodology
  - o The process
3. Penetration Testing
  - o What is Penetration Testing – An Introduction
  - o Why do you need a Penetration Test?
  - o Tools used in this process
4. Types of Attacks
  - o Eavesdropping
  - o Data Modification
  - o Identity Spoofing
  - o Password Based Attacks
  - o Denial of Service Attack
  - o Man in the Middle Attack
  - o Malicious Applets

5. Email Hacking – Demonstration

- o Overview
- o How it actually happens

6. Metasploit Demonstration

7. Security Objectives

- o The CIA Triad ; Data Confidentiality; Data Integrity;Data Availability
- o Security Guidelines

8. Intrusion Analysis

- o Prevention
- o Detection
- o Response and Recovery

9. Incident Preparation

- o Risk Management
- o Host Preparation
- o Network Preparation
- o Network Policies and Procedures
- o A response toolkit
- o The Incident Response Team

10. Risk Management

- o Asset Identification
- o Threat Identification
- o Vulnerability Analysis
- o Risk Analysis
- o Safeguard Selection
- o Security Monitoring

11. Why Do We Need Penetration Testers?

- o The problem
- o Some Statistics

12. Case Study: Putting it all together

13. The Million Dollar Question: Are you Secure?