

The Ultimate Network Penetration Class

COURSE DURATION: 5-days

CPE HOURS: 40

LEVEL: Advanced / Group-Live

PREREQUISITES: IT Audit & Security Boot Camp

ADVANCE PREPARATION: None

This class, taught by a member of the Canaudit Penetration Team, will teach you the skills and techniques required to identify, secure, and defend your network exposures. You will learn how to identify external and internal exposures, respond to security events, and secure the vulnerabilities. The external exposures consist of dialup connections; Internet based systems and devices, and wireless network connectivity. You will perform a war drive (*wireless network hunt*) in the local city area to identify inadequately secured wireless networks and how to properly secure them. You will also be attacking the Internet based systems, devices, and applications (routers, firewalls, switches, web servers, ftp servers, mail servers, VPN, and E-commerce applications) in an effort to get through the firewall and other protective measures, with the goal of full internal network access and ownership.

This class is constantly updated with the most current tools and exploits. Many tools required to perform a network penetration test will be loaded onto your machine during the class and are yours to keep.

This class can also be presented in-house. A major advantage of this approach is that it is a less expensive alternative to hiring an external team to conduct a penetration audit. As a class participant, you will conduct the audit in the classroom, with the instructor as your guide. Not only do you complete a penetration audit, but your employees learn new skills so that they can repeat the audit after the class.

WHO SHOULD ATTEND

This five-day hands-on class is designed for network security officers and IT auditors wanting to learn how to penetration test their organization's network. Some networking and O/S skills recommended.

SEMINAR OUTLINE

Day 1

- Intro and rules
- Installation of software & tools
- Testing of tools/ compatibility
- Review of ports & services
- Review of network infrastructure, primary network daemons, & distributed services
- Public information gathering
- Targeting of the organization's primary assets
- Creating attack strategies, techniques, & methodology

Day 2

- Focus on Windows based systems (NT, 2000, XP, 9x) with some Novell (4.x, 5.x)
- Explanation/ use of Windows specific tools to probe for weaknesses
- Network scanning & mapping
- Identification & explanation of high risk Windows systems exposures
- How to secure your Windows system
- Audit and security policies
- Windows best practices/test

Day 3

- Focus on Unix (System V, AIX, and Linux)
- Identification & explanation of high risk Unix exposures
- How to secure your Unix system
- Using Unix hacker/security tools to identify & exploit weaknesses
- Password cracking
- Unix security and auditing
- Unix best practices/test

Day 4

- Focus on war dialing and wireless networks
- Identification & explanation of primary dialup exposures
- Explanation and use of war dialing / driving tools
- How to secure your dialup connections
- Dialup best practices
- Conduct a war drive to identify insecure wireless networks
- Identification & explanation of high risk wireless exposures
- How to secure your wireless network
- Wireless best practices

Day 5

- Focus on routers, firewalls, switches, intrusion detection, & applying what you've learned
- Identification & explanation of firewall, router, and switch high risk exposures
- How to secure your network devices
- Network device & IDS best practices
- IDS software & techniques
- Honey pots and war games
- Preparing the audit report & exit interview (if time permits)
- Developing penetration plan for the next scheduled test

Participants must bring:

- A network enabled laptop/PC computer with a CD-ROM drive and a network card, as well as an Ethernet cable
- Windows NT4/2000/XP and/or Linux O/S is required
- Basic understanding of your O/S
- Office type suite which includes database & spreadsheet capabilities
- Local Administrator Rights