

# **Penetration Testing: Pre-emptive Network Security**

**COURSE DURATION:** 2-days

**CPE HOURS:** 16

**LEVEL:** Intermediate / Group-Live

**PREREQUISITES:** None

**ADVANCE PREPARATION:** None

This two-day seminar is designed for audit and security professionals. It teaches the necessary skills required for effective penetration testing. Participants will gain valuable insight into the most significant and common vulnerabilities and exploits that threaten their systems. The instructor will demonstrate the use of software tools and specialized techniques by conducting penetration tests on live sites and by analyzing past data. Participants will also have the opportunity to have their web sites tested during this session.

As corporate networks are linked together, pre-emptive security testing is a necessary protective mechanism. The Internet enables hackers to readily share new tools and exploits that threaten corporate security. Therefore it is essential that auditors and security professionals discover the network exposures before the hackers do. This seminar will provide the participants with a step-by-step approach that they can use to identify their vulnerabilities.

## **WHO SHOULD ATTEND**

This course is targeted towards auditors, system administrators, Information Technology personnel, and all others interested in the security of their company networks. This class is designed to increase the knowledge and awareness of participants of all levels.

## **SEMINAR OUTLINE**

### **I Identifying Your Assets**

- Customers
- Employees
- Company trade secrets
- World accessibility (fast global connections)
- Proprietary software
- Storage facility

### **II Who You Need to be Cautious Of and Why**

- Disgruntled employees
- Contractors, business partners, and trade associates
- Competitors
- Hackers
- Industrial Espionage Agents

### **III Security Basics**

- Policies and procedures
- Security Banners
- Log Files
- Anti-virus software
- Network security software
- Encryption

### **IV Frequently Exploited Ports and Services**

- Commonly exploited ports
- Email
- Flooding

### **V Tools of the Trade**

- Spoofing
- Network scanners
- Port scanners
- Demon dialers
- Password crackers
- Packet sniffers
- Miscellaneous tools

### **VI Hacking Your Network**

- Safe hacking
- Internet
  - Servers
  - Firewalls
  - Routers
- Dial up connections
  - NT
  - UNIX
  - Routers
  - Remote access software
- Physical security
  - Social engineering
  - Dumpster diving
- Intranet
  - Intranet vs. Internet
  - Mapping the network

### **VII Interpreting the Results**

- Immediate response and attention required
- Soon/fair response and attention required

- Moderate/minimal response and attention required

### **VIII Resolving the Issues**

- System Administrators (utilizing their abilities)
- Gaining management support
- Intruder response team (do you have one/how to create one)
- Applying skills to tasks

### **IX Pre-Emptive Security**

- Routine patch and software updates
- Random demon dialing
- Routine network scanning
- Routine log monitoring
- Future planning
- Continuing employee education

### **X Information and Tool Resources**

- Auditing
- Security
- Tool