

## Penetration Testing: Tools and Techniques - 4 Days

### Defending Your Network Using Hacking Techniques

*Course 537 Overview*

- You Will Learn How To**
- Deploy ethical hacking to expose weaknesses in your organization and select countermeasures
  - Gather intelligence by employing reconnaissance, published data and scanning tools
  - Probe and compromise your network using hacking tools to test and improve your security
  - Discover how malicious hackers exploit weaknesses to "own" the network
  - Protect against privilege escalation to prevent intrusions
  - Evade antivirus software, firewalls and IDS
- Course Benefits** As network breaches become increasingly sophisticated, proactive defenses are essential to counter malicious attacks. In this course, you learn to discover weaknesses in your network using the same mindset and methods as hackers. You acquire the knowledge to systematically test and exploit internal and external defenses. You learn countermeasures and how to reduce risk to your enterprise.
- Who Should Attend** Security consultants, Information Assurance auditors, firewall/IDS personnel, programmers, PCI security testers and those involved in cybersecurity measures and implementation. Security knowledge at the level of Course 468, "System and Network Security Introduction," and strong TCP/IP experience is assumed.
- Hands-On Training** Hands-on exercises model hacking methods and countermeasures, including:
- Preparing the hacker toolkit
  - Executing advanced port scanning
  - Linking vulnerabilities and exploits
  - Determining the vulnerabilities of a network
  - Performing injection attacks
  - Predicting and hijacking Web sessions
  - Poisoning DNS to lure clients
  - Configuring and using the Metasploit Framework
  - Defeating stateless firewalls, IDS and antivirus software
  - Cloning a Web site and stealing passwords

## Penetration Testing: Tools and Techniques - 4 Days

### Defending Your Network Using Hacking Techniques

*Course 537 Outline*

#### Introduction to Ethical Hacking

- Defining a penetration testing methodology
- Creating a security testing plan
- Adhering to PCI standards
- Assembling the hacking tools

#### Footprinting and Intelligence Gathering

##### Acquiring target information

- Locating useful and relevant information
- Scavenging published data
- Mining archive sites

##### Scanning and enumerating resources

- Identifying authentication methods
- Analyzing firewalls
- Harvesting e-mail information
- Interrogating network services
- Scanning from the inside out with HTML

#### Identifying Vulnerabilities

##### Correlating weaknesses and exploits

- Researching databases
- Determining target configuration
- Evaluating Vulnerability Assessment tools

##### Leveraging opportunities for attack

- Discovering exploit resources
- Attacking with Metasploit

#### Attacking Servers and Devices to Build Better Defenses

##### Bypassing router access control lists (ACLs)

- Discovering filtered ports
- Manipulating ports to gain access
- Connecting to blocked services

##### Compromising operating systems

- Examining Windows protection modes
- Analyzing Linux/UNIX processes

##### Subverting Web applications

- Injecting SQL and HTML code
- Hijacking Web sessions by prediction and fixation
- Bypassing authentication mechanisms

#### Manipulating Clients to Uncover Internal Threats

##### Baiting and snaring inside users

- Poisoning DNS
- Executing Cross-site scripting (XSS)
- Gaining control of browsers

##### Creating custom malware

- Harvesting client information
- Enumerating internal data

##### Deploying the Social Engineering Toolkit

- Cloning a legitimate site
- Diverting clients by poisoning DNS
- Delivering customized payloads to users

#### Exploiting Targets to Increase Security

##### Initiating remote shells

- Selecting reverse or bind shells
- Leveraging the Metasploit Meterpreter

##### Pivoting and island-hopping

- Deploying portable media attacks
- Routing through compromised clients
- Forwarding and redirecting ports

##### Pilfering target information

- Stealing password hashes
- Extracting infrastructure routing, DNS and NetBIOS data

##### Uploading and executing payloads

- Controlling memory processes
- Utilizing the remote file system

#### Testing Antivirus and IDS Security

##### Masquerading network traffic

- Obfuscating vectors and payloads
- Side-stepping perimeter defenses

##### Evading antivirus systems

- Falsifying file headers to inject malware
- Discovering the gaps in antivirus protection

#### Mitigating Risk and Next Steps

- Reporting results and creating an action plan
- Managing patches and configuration
- Recommending cybersecurity countermeasures
- Staying current with tools, trends and technology