NETWORK AND INFORMATION SECURITY TRAINING COURSES

www.tonex.com 1-888-to-tonex (1-888-868-6639)
International: 1-972-735-8686 Fax: 1-972-692-7492

Course Catalog 2011

TONEX Global Training Courses & Seminars

"Customization is Our Secret"

- Telecom
- IT Training
- Storage Networking
- Engineering
- Certification
- Workshop & Seminars
- Wireless Communication
- Business Management
- IP Networking
- Enterprise Architecture
- RF Engineering
- Boot Camps

Quality Training Delivered

NETWORK AND INTERNET SECURITY

6004 - Security Auditing and Attack Training

Duration: 2 Day(s)

This is the fourth course in a five part series that teaches students about the role of the security auditor, discovery methods that can be used to find weaknesses, auditing server penetration and attack techniques, and the steps of the control phase.

Objectives

- Identify auditing the security of a network.
- Identify the risk assessment process.
- Identify basic security-scanning techniques and enterprise-grade
- Auditing applications.
- Identify the categories of security information that help a security
- Auditor determines the security requirements of a network.
- Identify the network targets and related threats.
- Identify server penetration.
- Identify the control phase of auditing.
- Identify various hacking tools.

For detailed information: *www.tonex.com/Courses/6250/6004/*

6005 - IT Security Training Bootcamp

Duration: 5 Day(s)

Many organizations are now faced with the challenge of information exchange for its employees, suppliers, partners and customers. The Internet, World Wide Web, along with private networks has allowed this information to exchange more quickly than ever, but information exchange has not come without risk. With more reports of attacks against networks, IT managers are faced with the responsibility of protecting their data.

Tonex Security Boot camp covers Computer, Software & Network Security allows IT professionals, system and network administrators, incident handling team members, information assurance and audit professionals, the opportunity to gain knowledge and experience in various fields of computer and network security, intrusion detection, virtual private networks and security management.

This 5-day security boot camp, will teach you the language and underlying theory of computer, information and network security. The attendees will build on their knowledge and professional experience with computer and information security as they acquire the specific skills required to implement basic and advanced security services on

Objectives

TONEX Security Training Boot Camp covers:

- Network Penetration Testing
- Ethical Hacking
- Hacker Techniques, Exploits & Incident Handling
- Computer Forensics, Investigation, and Response
- Wireless Security Essentials
- Overview of Cryptography and Cryptanalysis
- Wireless Ethical Hacking, Penetration Testing, and Defenses
- Risk Assessment and Auditing
- Auditing Networks, Perimeters & Systems
- Host and Network Based Intrusion Detection
- Honey pots, Firewalls and Perimeter Protection
- Security Policy
- Password Management
- Security Incident Handling
- Information Warfare
- Web Security
- Network Fundamentals and TCP/IP Concepts
- Cisco Router Filters
- Primary Threats for Perimeter Protection
- PGP, Steganography
- Anti-Viral Tools
- Windows (2000, XP, 2003, Vista) Security Administration and Auditing
- UNIX Security Fundamentals
- Linux Security Administration and Auditing

For detailed information: *www.tonex.com/Courses/6250/6005/*

6006 - Certified Information Systems Security Professional (CISSP) Prep Training

Duration: 5 Day(s)

Our interactive, accelerated learning program prepares you for the CISSP exam. For experienced professionals in the computer security field who are responsible for developing the information security policies, standards, and procedures and managing their implementation across an organization.

This certification is the premier credential for security professionals pursuing higher levels of recognition and responsibility in the industry, and is seen as a requirement for many technical, midmanagement, and senior management positions.

Objectives

Upon completion of this program, you'll learn:

- Learn what you need to know to master the CISSP security technology
- Master Information Security skills by experts & get CISSP certified
- How to identify and correctly answer the any type of CISSP questions
- Important key test-taking tips for the CISSP exam
- Proven techniques for scoring high on the CISSP exam
- Important aspects of Security Policy development and Security Management Practices
- The goal of this course is to bring the CISSP® 10 domains of knowledge to life. By explaining important topics with stories, examples, and case studies, the practical workings of this information can be discovered.

We challenge you to attend the TONEX CISSP® training course and find the exciting aspect of the ten domains of knowledge.

For detailed information: *www.tonex.com/Courses/6250/6006/*

6016 - Intrusion Detection, Attacks & Countermeasures

Duration: 2 Day(s)

This course teaches you how to recognize the various stages of attacks and intrusions: scanning, exploits, elevation of privilege, Trojans and back doors. Every attack is different. The source of an attack might be an automated tool, a script kiddy, or a security expert working for a foreign government, and the source strongly affects the style and timing of the attack.

Objectives

- Identify vulnerable targets on your system
- Mitigate your security risks
- Recognize common and unusual attack patterns
- Create effective filters, honeypots, and firewalls
- Know and disable your enemies
- Recognize real detects versus false alarms, and know when to report them
- Set up your system to avoid false detects
- Evaluate ID systems and third-party tools
- Learn about automated response and manual response in relation to real-time analysis
- Propose and justify ID expenditures to management

For detailed information: *www.tonex.com/Courses/6250/6016/*

6018 - Enterprise PKI Fundamentals

Duration: 2 Day(s)

A public key infrastructure (PKI) is an increasingly critical component for ensuring privacy and authentication in an enterprise. This technology is capable of securing a wide range of applications across your organization. Successful PKI deployment requires detailed comprehension of many important issues. This hands-on course provides essential knowledge and skills needed to select, design and deploy a PKI to secure existing and future applications within your organization.

Objectives

Throughout this course, you gain extensive hands-on experience planning, designing and building a PKI. Exercises, performed under the guidance of an expert instructor, include:

- Analyzing PKI trust concepts
- Generating, using and validating digital signatures
- Building a Certification Authority and extending trust through PKI
- Integrating a PKI with existing directory systems
- Linking PKIs using cross-certification
- Identifying certificate components
- Integrating a PKI with applications
- Implementing a PKI solution to support a selected environment

For detailed information: *www.tonex.com/Courses/6250/6018/*

6019 - Virtual Private Network (VPN) Training

Duration: 2 Day(s)

VPN training includes VPN concepts and architectures, an in-depth examination of advanced features and functions such as tunneling, authentication, access control, VPN gateways, VPN clients, and VPN network and service management.

This course presents the various technology components, concrete solutions, and best practices you need to deploy and manage a highly successful VPN.

A VPN is a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed though some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis.

Virtual private networks have become an essential part of today's business networks, as they provide a cost-effective means of assuring private internal and external communications over the shared Internet infrastructure. Virtual Private Networks: Technologies and Solutions is a comprehensive, practical guide to VPNs.

Objectives

After completing this course, attendees will be able to:

- Understand IPsec, featuring the Authentication Header, Encapsulating Security Payload, Internet Key Exchange, and implementation details
- Understand PPTP, L2F, L2TP, and MPLS as VPN tunneling protocols
- Review Two-party and three-party authentication, including RADIUS and Kerberos
- Explore Public key infrastructure (PKI) concept and its integration into VPN solutions
- Understand Access control policies, mechanisms, and management, and their application to VPNs
- Review VPN gateway functions, including site-to-site intranet, remote access, and extranet
- Review Gateway configuration, provisioning, monitoring, and accounting
- Explore Gateway interaction with firewalls and routers
- Understand VPN client implementation issues, including interaction with operating systems
- Understand Client operation issues, including working with NAT, DNS, and link MTU limits
- Explore VPN service and network management architectures and tunnel and security management
- Review successful VPN deployments
- Discuss successful and unsuccessful VPN deployments
- Step through a practical process for managing a VPN deployment project
- Explore the current and future market trends

Prerequisites: Basic Knowledge of TCP/IP and Networking

For detailed information: *www.tonex.com/Courses/6250/6019/*

9004 - Security Training Boot Camp

Duration: 5 Day(s)

Many organizations are now faced with the challenge of information exchange for its employees, suppliers, partners and customers. The Internet, World Wide Web, along with private networks has allowed this information to exchange more quickly than ever, but information exchange has not come without risk. With more reports of attacks against networks, IT managers are faced with the responsibility of protecting their data.

Tonex Security Essential Bootcamp covers Computer, Software & Network Security allows IT professionals, system and network administrators, incident handling team members, information assurance and audit professionals, the opportunity to gain knowledge and experience in various fields of computer and network security, intrusion detection, virtual private networks and security management.

TONEX Security Essential Training Boot Camp at a glance:

- Network Penetration Testing
- Ethical Hacking
- Hacker Techniques, Exploits & Incident Handling
- Computer Forensics, Investigation, and Response
- Wireless Security Essentials
- Overview of Cryptography and Cryptanalysis
- Wireless Ethical Hacking, Penetration Testing, and Defenses
- Risk Assessment and Auditing
- Auditing Networks, Perimeters & Systems
- Host and Network Based Intrusion Detection
- Honeypots, Firewalls and Perimeter Protection
- Security Policy
- Password Management
- Security Incident Handling
- Information Warfare
- Web Security
- Network Fundamentals and TCP/IP Concepts
- Cisco Router Filters
- Primary Threats for Perimeter Protection
- PGP, Steganography
- Anti-Viral Tools
- Windows (2000, XP, 2003, Vista) Security Administration and Auditing
- Unix Security Fundamentals
- Linux Security Administration and Auditing

Objectives

After completing this course, attendees will be able to:

- Security Planning, Assessment, and Implementation
- Security Architecture and Models
- Availability, Integrity, and Confidentiality
- Security Management
- Cryptography Algorithms
- Cryptographic Attack and Defense Mechanisms
- Risk Management
- IT Security Auditing, Attacks, and Threat Analysis
- Operations Security
- Business Continuity Planning
- Intrusion Detection, Attacks and Countermeasures
- System Security
- Physical Security
- Access Control Systems
- Applications and Systems Security
- Firewalls
- Network and Web Security
- Security in SNMPv3 and IPv6
- Telecommunications Security
- Wireless Security
- Public Key Infrastructure
- Enterprise PKI
- Virtual Private Networks (VPN) Fundamentals
- Security Administration
- Law, Investigation and Ethics
- Security Policies, Standards, and Guidelines
- Computer crime laws and regulations

For detailed information: *www.tonex.com/Courses/6250/9004/*