Training Opportunity

Topic: Auditing Microsoft Windows Server and Active Directory Security

Dates & Times: April 9th | 8:00 am – 5:00 pm

April 10th | 8:00 am – 4:00 pm

Location: Sprint Nextel World Headquarters – Overland Park, Kansas
(Additional parking and building information will be provided to registered attendees)

CPE's: 16 Credits
*Please note actual CPE hours granted are dependent upon duration of speaker's presentation and may differ from advertised number of CPE hours.

Price: ISACA Members Early-Bird: $430 - Available for members today through March 29th.

ISACA Regular Members: $480 - Available for members from March 30th through April 5th.

Non-Members: $640 - Available for non-members today through April 8th.

Course Description
Microsoft is a major player in both the IT infrastructure and application development arenas. In this practical, information packed seminar, you will learn a structured approach to securing and auditing Microsoft servers and networking infrastructure, including Active Directory, from end-to-end and from top to bottom. You will cover all key Windows server control points, as well as common security risks, safeguards, and audit procedures. Forests, domains, directory services, Group Policy Object (GPO) control audit points and associated security and audit procedures within the Microsoft Active Directory architecture will be analyzed and demonstrated. Key changes affecting security and audit in different versions of Windows servers will be highlighted.

In this seminar, we will discuss:
- Windows Server roles and control points
- Security risks associated with Microsoft Windows Server and Active Directory
- Logical access controls within the Microsoft environment
- Local and domain security policies and group policy objects (GPOs)
- Microsoft TCP/IP applications and network services
- Domains, forests, and associated policy and trust relationships
- Types of Active Directory objects, domain controller roles, and user groups
- Windows Server and Active Directory management, security, and audit tools and techniques

Bonus: You will receive a comprehensive Windows Server and Active Directory Audit Data Collection Guide

Learning Objectives
- Identify the different versions and roles of Microsoft Windows servers and important differences in built-in security and auditability features
- Identify logical access control and other syst1em configuration parameters that affect the security of each Windows server and associated domain objects
- Locate sources of industry security and audit best practice guidance from Microsoft and other reputable resources
- Learn the basics of Lightweight Directory Access Protocol (LDAP) and its impact on Active Directory and Windows security policy deployment
- Gain familiarity with policy deployment and patch management
- Learn how to use built-in and low cost software tools to gather audit evidence and assess the level of security for Windows servers and Active Directory

Course Outline
Microsoft Windows Server and Active Directory Architecture
- Server roles and control points
- Variations among different versions of Windows Server
- Security risks associated with Microsoft Windows Server and Active Directory

Windows Server
- Windows Security Policies and Group Policy Objects (GPOs)
- User accounts
- User authentication
- Groups and privileged user authority
- Access control authorization
- Event logs and log management
- Microsoft TCP/IP applications and network services
- Tools, techniques, and references for auditing Windows server security

Active Directory
- Domains, forests, and associated policy and trust relationships
- Active Directory containers and network infrastructure
- Lightweight Directory Access Protocol (LDAP) design and security
- Types of Active Directory objects, domain controller roles, and user groups
- Domain user authentication protocols: NTLM, Kerberos
- Vulnerability and patch management
- Tools, techniques, and references for auditing Active Directory security

Windows Server and Active Directory Audit Planning and Scope
- Defining practical project scopes and sampling targets
- Review of audit evidence gathering procedures

Target Audience
IT Auditors; Information Security Managers and Analysts; IT Management; IT Architects; System Administrators; Compliance Officers; Consultants

Registration
Registration is available online: http://www.isaca-kc.org/meetingReg.php
Registration fees must be paid promptly following registration to secure your seat and course materials, if you are paying by check. Credit Card payment must be made at the time of registration.

Registration Includes
Course materials, morning coffee/water service, afternoon soft drink service and lunch provided onsite both days

Cancellation Policy
The Greater Kansas City Chapter of ISACA reserves the right to cancel the training seminar if the instructor is unable to attend, the facilities are not available, or other unforeseen circumstances arise. If this occurs, a reasonable effort will be made to reschedule the seminar or refunds will be issued. If a registrant cannot attend the seminar, the chapter requests an email notification two (2) weeks prior to the date of the event. Refunds will not be granted for cancellation requests received after this date. Generally, the chapter does not charge registrants a cancellation fee or penalty. Substitution of another individual for a confirmed registrant will be accepted at any time prior to the date of the event.

Speaker
Ken Cutler, CISA, CISSP, CISM, Security+, Senior Teaching Fellow – CPE Interactive (CPEi)
Ken is a Senior Teaching Fellow at CPEi (CPE Interactive), specializing in Technical Audits of IT Security and related IT controls. He is President and Principal Consultant of Ken Cutler & Associates (KCA) InfoSec Assurance, an independent consulting firm delivering a wide array of Information Security and IT audit professional consulting services. Mr. Cutler is also the Director – Professional Certification Programs for Security University.

Ken is an internationally recognized consultant and trainer in the Information Security and IT audit fields. He is both certified as and has conducted courses for: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) and CompTIA Security+. In cooperation with Security University, he recently was featured in two full length training videos on CISSP and Security+.

Formerly he was Vice President - Information Security for MIS Training Institute (MISTI) where responsibilities included: Information Security curriculum and advanced IT Audit course development, and chairing major IS and Business Continuity Planning (BCP) conferences and symposia.

Ken is a frequent and much-in-demand speaker on a wide array of IS and IT Audit topics. Through KCA, Mr. Cutler has personally delivered consulting services in both management and hands-on technical areas. He has also managed and directly participated in numerous Information Security consulting projects under various former MISTI affiliated professional services divisions, including the Information Security Institute (ISI) and Advanced Information Management (AIM).

Starting in 1993, Ken directed the development and growth of MISTI's IS curriculum and has frequently demonstrated his diverse expertise by personally developing and delivering numerous seminars and hands-on workshops in IS management and concepts, IT auditing, network infrastructure security and audit, web application security and audit, wireless security, and vulnerability testing. Since 1995, Mr. Cutler has frequently delivered hands-on network auditing and vulnerability testing courses in the United States, Russia, United Kingdom, Nigeria, South Africa, Serbia, Mexico, United Arab Emirates, Oman, and Greece. Audiences for his MISTI hands-on government technical auditing and security programs included: NASA, NIST, NSA, GSA, USDA, USPS, FDIC, and SSA.

He has lectured at many major industry and regional professional association events, including frequent appearances at numerous COMDEX shows in the United States, Canada, and Saudi Arabia from 1997-2002. Mr. Cutler has chaired the popular InfoSec Mexico program in partnership with EJ Krause from 2002-2010. Ken has been a featured speaker at the Middle East IT Security Conference (MEITSEC) in Dubai, UAE in 2002 and 2003.

His input on vulnerability testing tools is frequently sought out by major software vendors, such as IBM Internet Security Systems (ISS), Symantec (Axent), Hewlett-Packard (SPI Dynamics), NEMEA, Tenable, and The Saint Corporation.

Mr. Cutler has over 30 years of experience in IS, IT auditing, quality assurance, BCP, and information services. He has been performing different forms of IT Auditing projects and services since 1979. His industry experience includes: insurance, banking, financial services, natural resources, manufacturing, government contracting, security and audit software product design and utilization, consulting and training.

Ken has held numerous positions in IT management, including being the Chief Information Officer of a Fortune 500 company (Moore McCormack Resources) in the earlier stages of his professional career. He directed company-wide IS programs for American Express Travel Related Services, Martin Marietta Data Systems, and Midlantic Banks, Inc. The scope of his management responsibilities at those major corporations included: security policies and standards, awareness programs, security risk assessments, overseeing security administration, consulting services, and security technology selection. In response to the results of a series of his in-depth technical internal audits identifying major exposures in major application recoverability and data protection controls, he was appointed to form the Information Security program, including Disaster Recovery Planning, at Midlantic Banks, Inc. While at Midlantic Banks, he also served as the first President of the COMDISCO International Disaster Recovery Users Group. He represented American Express at the International Information Integrity Institute (I-4) and was unanimously elected by its members to serve on the I-4 Member Advisory Committee (MAC) during his first year of participation.

Ken has been a long-time active participant in international government and industry security standards initiatives including the President's Commission on Critical Infrastructure Protection, Generally Accepted System Security Principles (GSSP), Information Technology Security Evaluation Criteria (ITSEC), US Federal Criteria, and Department of Defense Information Assurance Certification Initiative.

Mr. Cutler is the primary author of the widely acclaimed Commercial International Security Requirements (CISR), which offers a commercial alternative to military security standards for system security design criteria. He is the co-author of the original NIST SP 800-41, "Guidelines on Firewalls and Firewall Policy". Ken has also published works on the intricacies of Information Security, security architecture, disaster recovery planning, wireless security, vulnerability testing, firewalls, single sign-on, and Payment Card Industry Data Security Standard (PCI DSS). In addition, he has been frequently quoted in popular trade publications such as *Computerworld*, *Information Security Magazine*, *Infoworld, InformationWeek, CIO Bulletin, Healthcare Information Security Newsletter, and MIS TransMISsion.* Mr. Cutler was featured in a special live TV program entitled, *"The Electronic Battlefield"*, on Abu Dhabi UAE Public TV and has also been interviewed on several US radio talk programs including *My Technology Lawyer and Talk America.*