2010 Spring Seminar

Topic: ESX Virtualization Security Audit & Assessment

Date: Thursday, February 25 and Friday, February 26, 2010

Time: 8:00 AM - 5:00 PM

Location: Sprint Nextel World Headquarters
6360 Sprint Parkway (Building 6360)
Overland Park, KS 66251
Phone (800) 701-3400

Parking: Parking Garage L

CPE’s: 16

Price: Early bird, ISACA member, $350 - through February 1, 2010
Regular, ISACA member, $400 - after February 1, 2010
Non-member, $530 – non-member registration opens February 12, 2010. Non-members may waitlist prior to February 12; however fees will not be accepted until non-member registration opens

Class Size: Limited to 20 participants (a second course may be offered if there is enough demand)

Required Materials: This is a “hands-on” course. Attendees are to bring the items noted below.

1. Laptop with administrator rights and Microsoft.NET installed, Putty-0.60 and WinSCP are also beneficial
2. Wireless and/or wired ethernet network connection capability
3. 25 ft or longer cat5 network cable if not using wireless (we have a limited number of loaners, please reserve in advance)

Seminar Information:
This two day course is designed to give the auditor or security assessor a background in the implementation of server virtualization, the risks associated with that implementation, control or security techniques to mitigate those risks, and approaches, tools, and techniques to assure that those controls and security tools are working as intended. The VMware ESX server is used to illustrate control or audit concepts because it is the most widely implemented virtualization software.

The hands-on portion of the class will require participants to install VMware Virtual Center client, also Windows Powershell and the Virtual Infrastructure Toolkit for Windows. **This software should be installed on a spare non-production laptop (or installed on your production laptop offline and removed before reconnection to your environment).** Each student should have administrative rights to install the software. Connectivity to the portable lab environment will either be achieved using a student provided long (25 ft or more) cat5 cable, or a wireless connection if the participant has an 802.11b wireless network capable card on their laptop.
Seminar Information (cont.):
Access point SSID & password and the student ID & password enabling access to the VMware Virtual Center Management Server using the client software will be assigned on-site. Microsoft .NET (dotnet) 2.0, WinSCP and Putty are also useful and free tools the student should pre-install on their machine before attending class, but those items also may be installed on-site.

Students will be provided a DVD containing class power points, open source client and other software, example assessment results, and a variety of vendor and other public domain reference material. Feedback to improve future deliveries of this content will be collected at the end of the class.

Registration:
Send an email to Registration@isaca-kc.org with the subject of “Spring 2010 ISACA KC Seminar Registration”. Upon receipt a confirmation and payment instructions will be provided to you in a separate email. Registration fees must be paid by February 19, 2010 to secure your seat and course materials.

Registration Includes:
Morning beverages (i.e., coffee and juice), lunch, afternoon snacks, and course materials on a DVD. More details about the lunch menus and refreshments will be forthcoming.

Instructor:
Michael T. Hoesing CISA, CISSP, CCP, CIA, CFSA, CMA, CPA, ACDA

Bio:
Mike has over 30 years of experience in the areas of information systems audit and assurance, information systems implementation, and financial audit. His experiences span a variety of industries during his years with public accounting firms and his last 18 years has focused on the financial services with firms such as First Data Corp, First National Nebraska Inc., Pricewaterhouse Coopers, and American Express. Mike has been involved in both the external and internal audit processes and also has served as a software trainer.

Mike has been a conference speaker at the Computer Security Conference, VMworld, ISACA’s CACS, IIA Midwest Regional, RSA Executive Security Action Forum, and the CERT and InfoTec conferences covering ESX risk, security and assessment techniques. In March 2010 Mike is scheduled to present on Virtualization Security Assessments at the RSA conference.

Mike has been published in the Information Systems Control Journal published by ISACA on network security, operating systems and virtualization risk and audit topics. Contributions to team documents include the FSR/BITS Information Technology Outsourcing Framework document and the Center for Internet Security Virtualization and ESX Server benchmarks. In May 2009 his Virtualization Security Assessment Tools and Techniques article has been published in the Information Security Journal: A Global Perspective published by ISC².
Bio (cont.):
Mike has lead the Information Systems Audit and Information Assurance groups for various
organizations conducting traditional IS and integrated audit activities, along with proactive
control and risk management consulting, technical assessments, forensics, eDiscovery litigation
support, and external assessment liaison with regulatory, financial and credit card association
assessors, evaluating risk and helping to improve the control environment for all technology
teams.

Mike developed the first Virtualization audit class delivered to ISACA chapters and presented
the 2 day version of that class at MISTI's InfoSec World Conference in March 2009.

University involvement includes membership on the Creighton University and University of
Nebraska at Omaha College of Business advisory boards, and facilitating sessions in Creighton’s
eSecurity lab. At the University of Nebraska at Omaha, he developed and delivers the regions
only class devoted to Information Systems Audit following the ISACA model curriculum and
has enrolled that school in the ACL and VMware beta partner programs. He is a board member
of NebraskCERT, the area’s leading information security professional group.

Agenda – 2 Day Course
(Times and topics are approximate for this rapidly developing subject matter)

Day 1
8:00 - 8:35 Registration, Software Installation

8:30 - 9:30 Background (60 minutes)
  1. Introductions, Logistics, Attendee’s Learning Objectives
  2. Virtualization Resources, Course CD, have a printed copy of the audit program available
  3. Virtualization Background, History
  4. Virtualization Benefits
  5. Virtualization as a Control or Security Enhancer
  6. Virtualization Approaches, Vendors, Definitions
  7. Current Developments
  8. General Risks
  9. Applying Virtualization in IS Audit, and in IS Audit Education
 10. Lab Configuration
 11. VMworld, VMware Security Lab, VCP

9:30 - 10:30 Overall Risks and Standards (60 minutes)
  12. 10 Key Risks
  13. Gartner Risk Research Results
  14. Other Risk Perspectives, article, blogs, vendors
  15. Standards – Center for Internet Security (3.0 2007, 3.5 in 2009)
  16. Standards - VMware Whitepapers (3.5 2008)
  17. Standards - DISA STIG (final 2008)
  18. Vulnerabilities - VMSA’s and CVE’s
  19. Hardware Risks
Agenda (cont.):

Day 1

10:30 - 10:40 break

10:40 - 12:00 ESX 3.5 Update 3 = Controls and Security Techniques, Network Configuration & User Access (80 minutes)
   20. Default Setting “High” (2.x and 3.x)
   21. Remote Connections (through vCenter, client direct, web direct)
   22. Network Configurations and Commands
   23. Ports, SNMP, VLANs, Other
   24. Forwards and Redirects
   25. Iptables Firewall (3.x, not in 2.x)
   26. COS Root & VC Administrator controls
   27. Virtual Center Roles & Users
   28. Password Configuration

12:00 - 1:00 lunch

1:00 - 1:45 Configuration and Other; Risks and Controls (45 minutes)
   29. Patches (VMware not RHEL), VMware Update Manager
   30. Storage Options & Considerations (redundancy, access)
   31. Resource Allocation & DOS
   32. Command Line Tools
   33. Logging & Monitoring
   34. Data Discovery
   35. Other

1:45 - 2:30 ESX Audit/Assessment Approaches and Tools (45 minutes)
   36. Specific Metric Comparison and Enumeration Approaches
   37. Nontechnical Tools and Scope Topics
   38. Tools – Free (or nearly free)
   39. Tools – Vendor Solutions
   40. ESX Policy
   41. ESX Audit Program

2:30 - 2:40 break

2:40 - 4:30 Hands-On (where affordable and logistically possible) Application of Tools to one Risk – Unassociated (rogue) Guests (110 minutes)
   42. Free Tools –
      (Bastille, LSAT, instructors script do not collect metrics on this topic)
      CLI and esxcfg-xxx commands,
      VMware VI Toolkit for Windows and Microsoft PowerShell

   43. Marginally Free Tools –
      vCenter Management Server, CIS-CAT for members
2010 ISACA Greater Kansas City Spring Seminar
ESX Virtualization Security Audit & Assessment

Agenda (cont.):
Day 1

44. Vendor Tools -
   Reflex (discovery)
   Ecora
   Tripwire
   Configuresoft
   V-Commander
   esxcfg-info read into ACL data analytics tool

Day 2
Executing the ESX 3.5 Update 3 Security and Control Audit Program Start to Finish

8:30 - 10:00 Hands-On Network Assessment (90 minutes)
   1. Interviewing, Network Diagrams, Configuration Standards, InfoSec Policy
   2. Virtual Center Management Console
   3. COS (CLI) esxcfg-xxx commands
   4. Other Free tools (Bastille, LSAT, Instructors bash script)
   5. External Tools – nmap, Nessus

10:00 – 10:10 break

10:10 – 12:00 Hands On - ESX Configuration, Access (110 minutes)
   6. Virtual Center Management Console
   7. COS (CLI) esxcfg-xxx commands

12:00 – 1:00 lunch

1:00 – 2:30 Other Audit/Assessment procedures (90 minutes)
   8. Logging
   9. Patching (VMware Update Manager)
   10. Security products and placement
   11. Storage considerations
   12. Build your own tools – VI SDK/API (Perl)
   13. ESXCFG-INFO
   14. Other Tools – Veeam, vCommander, SearchMyVM, miscellaneous

2:30 – 2:40 break

2:40 – 4:30 Misc Topics, QA, Other, Attendee Defined Tests (110 minutes)

15. 2:40 – 3:00 PCI/DSS Considerations (20 minutes)
16. 3:00 – 3:15 ESX Versions Before 3.5 (15 minutes)
17. 3:15 – 3:30 Backup and continuity topics (15 minutes)
18. 3:30 – 4:30 Q&A, references, student defined testing, other virtualization products, other (60 minutes)