SANS Boston 2010

Boston, MA • August 2 - 8, 2010

The Most Trusted Name in Information and Software Security

Hands-on immersion training programs in:

SANS Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

SANS Security Leadership Essentials For Managers

Web App Penetration Testing and Ethical Hacking

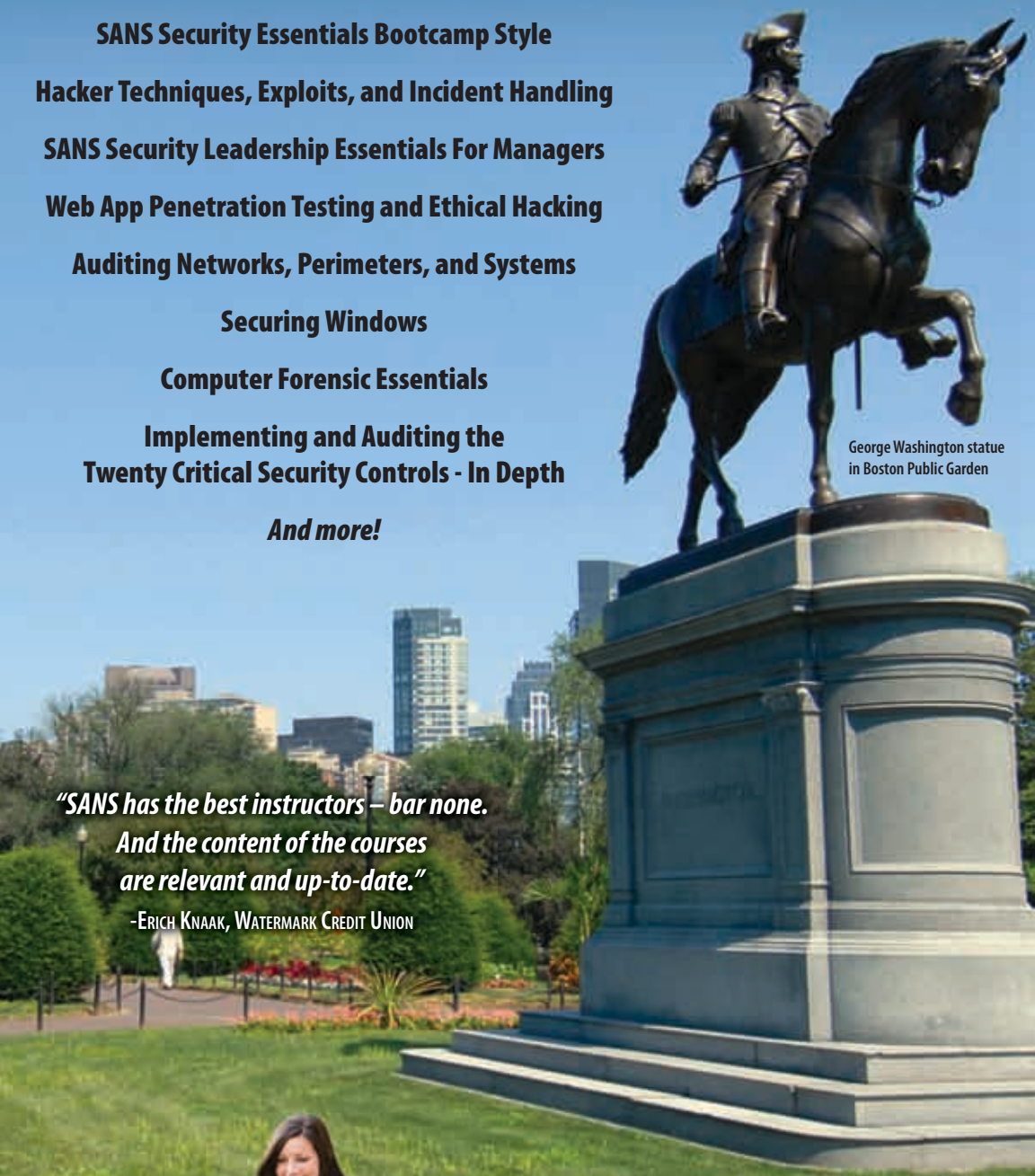
Auditing Networks, Perimeters, and Systems

Securing Windows

Computer Forensic Essentials

Implementing and Auditing the Twenty Critical Security Controls - In Depth

And more!



George Washington statue in Boston Public Garden

"SANS has the best instructors – bar none. And the content of the courses are relevant and up-to-date."

-Erich Knaak, Watermark Credit Union

Register at www.sans.org/boston-2010

GIAC Approved Training

Dear Colleague,


Stephen Northcutt

I am excited to invite you to experience both the past and the future with Boston's great historic culture and our cutting-edge security training. Don't miss the chance to gain in-depth knowledge that you will use the minute you get back to your office. With eight 5- and 6-day courses in Audit, Management, Security, and Forensics, we have something for everyone!

A look through this brochure reveals that SANS Boston 2010 offers top-rated courses brought to you by Dr. Eric Cole, Dave Shackleford, John Strand, Jason Fossen, David Hoelzer, Tanya Baccam, Chad Tilbury, and me! We are also offering three one-day, skills-based courses to pack your week with the most current security information available anywhere. This brochure will tell you about the DoD 8570 Directive, and you can find out which SANS courses align. See the GIAC page to learn about getting GIAC Certified! Use the Roadmap to plan your career.

Add depth to your training experience with our special and unique evening events, including:

- **Welcome to SANS with Eric Cole, PhD.**
- **Community of Interest in Networking and Security (COINS) Vendor Reception – Stephen Northcutt**
- **Rapid Response Security Strategy Competition (RRSSC)**
- **Shabu Zen White T-shirt Contest**
- **GIAC Program Overview and SANS Technology Institute Brief – Stephen Northcutt**

Last year's attendees had this to say about their experience at SANS Boston 2009:

"Another day in another outstanding SANS class under the tutelage of another amazing instructor." -Jim Medeiros, MIT – Lincoln Labs

"It's just awesome – I have stuff to bring back to coders and designers why they must do three things: patch, harden, and learn what hackers do against their 'secure' systems." -Matthew Coles, EMC/RSA

Join us at the Hyatt Regency Boston which is just one block from the Boston Common. Take a walk to experience downtown Boston with its shopping, theaters, and Chinatown. For a huge amount of information about Boston and things to do there, check out our Insiders Guide to Boston at www.sans.edu/resources/musings/sansboston_2010.php

Register by June 23 to receive a $400 tuition fee discount as well! Start making your training and travel plans now and let your colleagues and friends know about SANS Boston 2010. We look forward to seeing you there.

Best regards,

Stephen Northcutt
President
SANS Technology Institute, a postgraduate computer security college

Courses-at-a-Glance

	MON 8/2	TUE 8/3	WED 8/4	THU 8/5	FRI 8/6	SAT 8/7	SUN 8/8
AUD507 Auditing Networks, Perimeters, and Systems	PAGE 4						
MGT305 Technical Communication & Presentation Skills for Security Professionals							PG 12
MGT421 SANS Leadership and Management Competencies						PG 12	
MGT512 SANS Security Leadership Essentials for Managers	PAGE 5						
SEC401 SANS Security Essentials Bootcamp Style	PAGE 6						
SEC504 Hacker Techniques, Exploits & Incident Handling	PAGE 7						
SEC505 Securing Windows	PAGE 8						
SEC517 Cutting-Edge Hacking Techniques							PG 12
SEC542 Web App Penetration Testing and Ethical Hacking	PAGE 9						
SEC566 Implementing and Auditing the 20 Critical Security Controls - In Depth	PAGE 10						
FOR408 Computer Forensic Essentials	PAGE 11						

Please check the Web site for an up-to-date course list at www.sans.org/boston-2010

SANS TRAINING AND YOUR CAREER ROADMAP

SECURITY CURRICULA

Incident Handling Curriculum

SEC501 Advanced Security Essentials – Enterprise Defender *GCED*

SEC504 Hacker Techniques, Exploits, and Incident Handling *GCIH* *Page 7*

FOR508 Computer Forensic Investigation and Incident Response *GCFA*

Additional Incident Handling Courses

SEC517: Cutting-Edge Hacking Techniques *Page 12*

SEC550: Information Reconnaissance: Competitive Intelligence and Online Privacy

Beginners

SEC301 Intro to Information Security *GISF*

SEC401 SANS Security Essentials Bootcamp Style *GSEC* *Page 6*

SEC301 NOTE:
If you have experience in the field, please consider our more advanced course – SEC401.

Intrusion Analysis Curriculum

SEC501 Advanced Security Essentials – Enterprise Defender *GCED*

SEC502 Perimeter Protection In-Depth *GCFW*

SEC503 Intrusion Detection In-Depth *GCIA*

Additional Intrusion Analysis Courses

SEC577: Virtualization Security Fundamentals

Penetration Testing Curriculum

SEC540 VoIP Security

SEC542 Web App Pen Testing and Ethical Hacking *GWAPT* *Page 9*

SEC560 Network Pen Testing and Ethical Hacking *GPEN*

SEC617 Wireless Ethical Hacking, Pen Testing, and Defenses *GAWN*

SEC709 Developing Exploits for Pen Testers and Security Researchers

Additional Penetration Testing Courses

DEV538: Web Application Pen Testing

SEC553: Metasploit for Pen Testers

SEC561: Network Penetration Testing

SEC567: Power Packet Crafting with Scapy

Network and Application Security Curriculum

SEC501 Advanced Security Essentials – Enterprise Defender *GCED*

Additional Network and Application Security Courses

SEC440: 20 Critical Security Controls: Planning, Implementing, and Auditing

SEC556: Comprehensive Packet Analysis

SEC566: Implementing and Auditing the 20 Critical Security Controls – In Depth *Page 10*

SEC565: Data Leakage Prevention - In Depth

System Administration Curriculum

SEC501 Advanced Security Essentials – Enterprise Defender *GCED*

SEC505 Securing Windows *GCWN* *Page 8*

SEC506 Securing Linux/Unix *GCUX*

Additional System Administration Courses

SEC434: Log Management In-Depth

SEC509: Securing Oracle

SEC531: Windows Command-Line Kung Fu

SEC546: IPv6 Essentials

SEC564: Hacker Detection for System Administrators

FORENSICS CURRICULUM

FOR408 Computer Forensic Essentials *Page 11*

FOR508 Computer Forensic Investigation and Incident Response *GCFA*

FOR558 Network Forensics

FOR563 Mobile Device Forensics

FOR610 REM: Malware Analysis Tools & Techniques *GREM*

Additional Forensics Courses

FOR526: Advanced Filesystem Recovery and Memory Forensics

APPLICATION SECURITY CURRICULUM

Web App Security

DEV522 Defending Web Applications Security Essentials

Web App Pen Testing

SEC542 Web App Pen Testing and Ethical Hacking *GWAPT* *Page 9*

Additional Web App Pen Testing Courses

DEV538: Web App Pen Testing

Secure Coding

DEV541 Secure Coding in Java/JEE: Developing Defensible Apps *GSSP-JAVA*

DEV544 Secure Coding in .NET: Developing Defensible Apps *GSSP-.NET*

DEV545 Secure Coding in PHP: Developing Defensible Apps

Additional Secure Coding Courses

DEV304: Software Security Awareness

DEV320: Introduction to the Microsoft Security Development Lifecycle

DEV534: Secure Code Review for Java Web Apps

DEV536: Secure Coding for PCI Compliance

DEV543: Secure Coding in C & C++: Developing Defensible Applications

AUDIT CURRICULUM

SEC301 Intro to Information Security *GISF*

SEC401 SANS Security Essentials Bootcamp Style *GSEC* *Page 6*

AUD507 Auditing Networks, Perimeters, and Systems *GSNA* *Page 4*

Additional Audit Courses

AUD410: IT Security Audit and Control Essentials

AUD429: IT Security Audit Essentials Bootcamp

AUD521: PCI/DSS 1.2: Becoming and Staying Compliant

SEC440: 20 Critical Security Controls: Planning, Implementing, and Auditing

SEC566: Implementing and Auditing the 20 Critical Security Controls - In Depth *Page 10*

LEGAL CURRICULUM

SEC301 Intro to Information Security *GISF*

SEC401 SANS Security Essentials Bootcamp Style *GSEC* *Page 6*

LEG523 Legal Issues in Information Technology and Information Security *GLEG*

GIAC certification available for courses indicated with GIAC acronyms

MANAGEMENT CURRICULUM

SEC301 Intro to Information Security *GISF*

MGT512 SANS Security Leadership Essentials For Managers with Knowledge Compression™ *GSLC* *Page 5*

SEC301 Intro to Information Security *GISF*

MGT414 SANS® +S™ Training Program for the CISSP® Certification Exam *GISP*

SEC401 SANS Security Essentials Bootcamp Style *GSEC* *Page 6*

MGT525 Project Management and Effective Communications for Security Professionals and Managers *GCPM*

Additional Management Courses

MGT305: Technical Communication and Presentation Skills for Security Professionals *Page 12*

MGT404: Fundamentals of Information Security Policy

MGT411: SANS 27000 Implementation & Management

MGT421: Leadership and Management Competencies *Page 12*

MGT432: Information Security for Business Executives

MGT438: How to Establish a Security Awareness Program

For a complete list of SANS courses, visit www.sans.org.

For a complete list of GIAC Certifications, visit www.giac.org.

DoD Directive 8570 requires:

By the end of CY 2010, ALL personnel performing IAT and IAM functions must be certified.

By the end of CY 2011 ALL personnel performing CND-SP and IASAE roles must be certified.

ALL IA jobs will be categorized as 'Technical' or 'Management' Level I, II, or III, and to be qualified for those jobs, you must be certified.

"It's not about the cert, it's about the knowledge gained in pursuit of the cert."

-Dave Hull,
Trusted Signal, LLC

DoD Baseline IA Certifications

TECH II: GSEC TECH III: GCIH • GSE • CISSP • CISA
MGT I: GSLC • GISF MGT II: GSLC • CISSP MGT III: GSLC • CISSP

Information Assurance System Architecture & Engineering (IASAE) Certifications

IASAE I: CISSP IASAE II: CISSP

Computer Network Defense (CND) Certifications

CND Analyst: GCIA CND Incident Responder: GCIH CND Auditor: GSNA • CISA

Training for Certifications

AUD423: CISA AUD507: GSNA MGT414: CISSP MGT512: GSLC SEC301: GISF
SEC401: GSEC SEC503: GCIA SEC504: GCIH SEC401, SEC503 & SEC504: GSE

Get more information at www.sans.org/8570

Global Information Assurance Certification

EARN YOUR CERTIFICATION

Top Four Reasons to 'Get GIAC Certified'

1. ***Promotes*** **hands-on technical skills and improves knowledge retention**

   "The GIAC certification process forced me to dig deep'er into the information that I was taught in class. As a result of this, I integrated this training into my practical skill set and improved my hands-on skills." -Dean Farrington, Information Security Engineer, Wells Fargo

2. ***Provides*** **proof that you possess hands-on technical skills**

   "GIAC proves that I have a very solid technical background to support any challenge I deal with every day. There are so many new tools coming up daily, but the underlying background essentially remains the same." -Wayne Ho, Business Information Security Officer, Global Bank

3. ***Positions*** **you to be promoted and earn respect among your peers**

   "I think the GIAC certification has definitely helped provide credibility for me in the workplace. This, in turn, has helped me be more effective at my job." -Matt Austin, Senior Security Consultant, Symantec

4. ***Proves*** **to hiring managers that you are technically qualified for the job**

   "Hiring managers are always looking for ways to help sort through candidates. GIAC certifications are a major discriminator. They ensure that the candidate has hands-on technical skills." -Chris Schock, Network Engineer, State of Colorado

AUDIT
507

Auditing Networks, Perimeters, and Systems

Six-Day Program • Mon, August 2 - Sat, August 7, 2010 • 9:00am - 5:00pm
36 CPE Credits • Laptop Required • Instructor: David Hoelzer

CND Auditor for the Department of Defense Baseline Certification for 8570

Who Should Attend

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on IT auditing
- Managers responsible for overseeing the work of an IT audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how they think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise.

What systems really matter? How do we prioritize the audits that need to be performed and determine the scope of each? How do you validate the security of the perimeter? What settings should be checked on the various systems under scrutiny? Which set of processes can be put into place to allow an auditor to focus on the business processes rather than the security settings?

This course is organized specifically to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering high-level audit issues and general audit best practice, students will have the opportunity to dive into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will come from real-world examples.

One of the struggles that IT auditors face is helping management understand the relationship between the technical controls and the risks to the business. The instructor will use validated information from real-world situations to explain how they can be used to raise the awareness of management and others within the organization to understand why these controls specifically, and auditing in general, is important. Each student is invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMware Fusion.

A great audit is more than marks on a checklist; it is the understanding of the underlying controls, knowing what the best practices are, and having enough information to understand why. Sign up for this course and experience the mix of theory, hands-on, and practical knowledge.

Get GSNA Certified

Reinforce what you learned in training and prove your skills and knowledge with a GSNA certification.
www.giac.org

MSISM
www.sans.edu

Register at www.sans.org/boston-2010

David Hoelzer *SANS Faculty Fellow*

With more than twenty years of experience, David has served in positions ranging from the highly technical to senior management for a variety of organizations. For the last ten years, David has been the director of research for Cyber-Defense and the principal examiner for Enclave Forensics. In addition to day-to-day responsibilities, he has acted as an expert witness for the Federal Trade Commission and continues to teach at major SANS events, teaching security professionals from organizations including NSA, USDA Forest Service, Fortune 500 security engineers and managers, DHHS, various DoD sites, national laboratories, and many colleges and universities. From time to time David also speaks nationally and internationally on various security topics.

SANS Security Leadership Essentials for Managers with Knowledge Compression™

MANAGEMENT 512

Five-Day Program • Mon, August 2 - Fri, August 6, 2010
9:00am - 6:00pm (Days 1-4), 9:00am - 4:00pm (Day 5)
33 CPE Credits • Instructor: Stephen Northcutt

IAM Levels I, II, and III of the Dept. of Defense Baseline Certification for 8570

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology.

You don't just learn about security, you learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Papers 800 guidance so that it can be particularly useful to US government managers and supporting contractors.

Essential security topics covered in this management course include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, Web application security, offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security + 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Who Should Attend

- This course is designed and taught for mid-level to C-level managers and leaders. It will give you the ability to better manage IT projects in a secure manner.
- Anyone with 8570 information assurance management responsibilities
- Senior executives
- Vice presidents
- Security or assurance officers and managers
- Upwardly mobile managers

This course is taught MBA style, and students are expected to be ready to work on the in-class exercises by preparing prior to the first day of instruction. When you enroll in MGT512, we suggest you review the following items before the course begins:

- PAAG Template
- BITS Kalculator
- 7799 Checklist
- SANS Security Policy Project
- Security Incident Handling Forms

Please note that some course material for SEC401 and MGT512 may overlap. We recommend SEC401 for those interested in a more technical course of study and MGT512 for those primarily interested in a leadership-oriented but less technical learning experience.

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and currently serves as President of the SANS Technology Institute, a post graduate level IT Security College, www.sans.edu. Stephen is author/coauthor of *Incident Handling Step-by-Step, Intrusion Signatures and Analysis, Inside Network Perimeter Security* 2nd Edition, *IT Ethics Handbook, SANS Security Essentials, SANS Security Leadership Essentials*, and *Network Intrusion Detection* 3rd edition. He was the original author of the Shadow Intrusion Detection system before accepting the position of Chief for Information Warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer.

Get GSLC Certified

Reinforce what you learned in training and prove your skills and knowledge with a GSLC certification.

www.giac.org

MSISM
www.sans.edu

SECURITY
401

SANS Security Essentials Bootcamp Style

Six-Day Program • Mon, August 2 - Sat, August 7, 2010
46 CPE Credits • 9am - 7pm (Days 1-5), 9am - 5pm (Day 6)
Laptop Required • Instructor: Dave Shackleford

IAT Level II & III of the Dept. of Defense Baseline Certification for 8570

This course is endorsed by the Committee on National Security Systems (CNSS) NSTISSI 4013 Standard for Systems Administrators in Information Systems Security (INFOSEC).

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Network engineers wanting to enter the field of security
- Security engineers, admins, managers, and others wanting a more detailed understanding of the technical components of security
- Anyone new to information security with some background in information systems and networking
- Individuals with operational responsibility for a firewall, VPN, or Internet-facing device

Maximize your training time and turbo-charge your career in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification.

Security Essentials is designed to give anyone interested in network security the skills required to be an effective player in this arena. This in-depth, comprehensive course provides the essential, up-to-the-minute knowledge and skills required for securing systems and organizations, and equips you with the language and theory of computer security. Learn all of this and more from the best security instructors in the industry.

B O O T C A M P

Security 401 PARTICIPANTS ONLY
*5:15pm - 7:00pm - **Required** — Course Days 1-5*

Attendance is required for the evening bootcamp sessions as the information presented appears on the GIAC exams. These daily bootcamps give you the opportunity to apply the knowledge gained throughout the course in an instructor-led environment. It helps fill your toolbox with valuable tools you can use to solve problems when you go back to work. The material covered is based on Dr. Eric Cole's "cookbook for geeks," and most students find it to be one of the highlights of their Security Essentials experience! Students will have the opportunity to install, configure, and use the tools and techniques they have learned. CDs containing the software required will be provided for each student. Students should arrive with a laptop properly configured. A working knowledge of each operating system is recommended but not required. For students who do not wish to build a dual boot machine, SANS will provide a bootable Linux CD for the Linux exercises.

Get GSEC Certified

Reinforce what you learned in training and prove your skills and knowledge with a GSEC certification.

www.giac.org

MSISE
www.sans.edu

Dave Shackleford *Certified Instructor*

Dave Shackleford, Director of Security Assessments and Risk & Compliance at Sword & Shield Enterprise Security, is a SANS Analyst, instructor and GIAC technical director. He has consulted with hundreds of organizations in the areas of regulatory compliance, security, and network architecture and engineering. He's worked as CSO for Configuresoft, CTO for the Center for Internet Security, and has also worked as a security architect, analyst, and manager for several Fortune 500 companies.

Hacker Techniques, Exploits, and Incident Handling

SECURITY 504

Six-Day Program • Mon, August 2 - Sat, August 7, 2010 • 9:00am - 5:00pm
36 CPE Credits • Laptop Required • Instructor: John Strand

IAT Level III and CND Analyst for the Dept. of Defense Baseline Certification for 8570

Who Should Attend

- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

If your organization has an Internet connection or a disgruntled employee (and whose doesn't!), your computer systems will get attacked.

From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets to the spyware your otherwise wholesome users inadvertently downloaded, attackers are targeting your systems with increasing viciousness and stealth.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, the in-depth information helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the 'oldie-but-goodie' attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. This workshop also includes the unique SANS Capture-the-Flag event on the last day where you will apply your skills developed throughout the session to match wits with your fellow students and instructor in a fun and engaging learning environment. You'll get to attack the systems in our lab and capture the flags to help make the lessons from the whole week more concrete. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

John Strand *Certified Instructor*

John Strand currently is the owner and senior security researcher with Black Hills Information Security, and a consultant with Argotek, Inc for TS/SCI programs. As a certified SANS instructor, he teaches SEC504, SEC517, and SEC560. He is a contributing author of *Nagios 3 Enterprise Network Monitoring*, and a regular contributor to *SearchSecurity's Ask the Expert* series on the latest information security threats. He also regularly posts videos demonstrating the latest computer attacks and defenses at vimeo.com/album/26207. He started the practice of computer security with Accenture Consulting in the areas of intrusion detection, incident response, and vulnerability assessment/penetration testing. John then moved on to Northrop Grumman specializing in DCID 6/3 PL3-PL5 (multi-level security solutions), security architectures, and program certification and accreditation. He has a master's degree from Denver University and is currently also a professor at Denver University. In his spare time he writes loud rock music and makes various futile attempts at fly-fishing.

Get GCIH Certified

Reinforce what you learned in training and prove your skills and knowledge with a GCIH certification.
www.giac.org

MSISE
www.sans.edu

Register at www.sans.org/security-west-2010

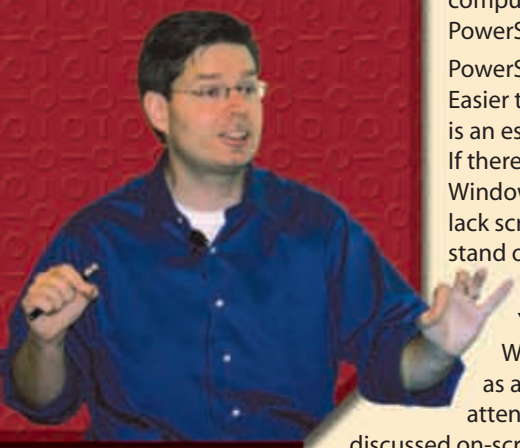
SECURITY
505

Securing Windows

Six-Day Program • Mon, August 2 - Sat, August 7, 2010 • 9:00am - 5:00pm
36 CPE Credits • Laptop Required • Instructor: Jason Fossen

Who Should Attend

- Windows network security engineers and architects
- Windows administrators with security duties
- Anyone with Windows machines who wants to implement the SANS 20 Critical Security Controls
- Active Directory designers and administrators
- Those who must enforce security policies on Windows hosts
- Those deploying or managing a PKI or smart cards
- IIS administrators and Web masters with Web servers at risk
- Administrators who use the command line or scripting to automate their duties and must learn PowerShell (the replacement for CMD scripting and VBScript)



Get GCWN Certified

Reinforce what you learned in training and prove your skills and knowledge with a GCWN certification.

www.giac.org

Will you be transitioning from Windows XP to Windows 7?

The Securing Windows course is fully updated for Windows Server 2008-R2 and Windows 7. Most of the content applies to Windows Server 2003 and XP too, but the focus is on 2008/Vista/7.

Concerned about the 20 Critical Security Controls of the Consensus Audit Guidelines? This course will help you implement the Critical Controls relevant to Windows systems, not just audit them, and will walk you through most of the tools step-by-step, too.

As a Windows security expert, how can you stand out from the crowd and offer management more than the usual apply-this-checklist advice? Be a security architect who understands the big picture. You can save your organization money, maintain compliance with regulations, secure your networks, and advance your career all at the same time. How? By leveraging the Windows infrastructure you've already paid for.

This program is a comprehensive set of courses for Windows security architects and administrators. It tackles tough problems like Active Directory forest design, how to use Group Policy to lock down desktops, deploying a Microsoft PKI and smart cards, pushing firewall and IPSec policies out to every computer in the domain, securing public IIS Web servers, and PowerShell scripting.

PowerShell is the future of Windows scripting and automation. Easier to learn and more powerful than VBScript, PowerShell is an essential tool for automation and scalable management. If there is a one skill that will most benefit the career of a Windows specialist, it's scripting. Most of your competition lack scripting skills, so it's a great way to make your resume stand out. Scripting skills are also essential for being able to implement the 20 Critical Security Controls.

You are encouraged to bring a virtual machine running Windows Server 2008 Enterprise Edition configured as a domain controller, but this is not a requirement for attendance since the instructor will demo everything discussed on-screen. You can get a free evaluation version of Server 2008 from Microsoft's Web site (just do a Google search on "site:microsoft.com Server 2008 trial"). You can use VMware, Virtual PC or any other virtual machine software.

This is a fun and fascinating course, a real eye-opener even for Windows administrators with years of experience. Come see why there's a lot more to Windows security than just applying patches and changing passwords; come see why a Windows network needs a security architect.

Jason Fossen *SANS Faculty Fellow*

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS' week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS' projects since 1998. He graduated from the University of Virginia, received his master's degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas.

Web App Penetration Testing and Ethical Hacking

SECURITY 542

Six-Day Program • Mon, August 2 - Sat, August 7, 2010 • 9:00am - 5:00pm
36 CPE Credits • Laptop Required • Instructor: Tanya Baccam

Assess Your Web Apps In Depth.

Web applications are a major point of vulnerability in organizations today. Web app holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited Web sites altered by attackers. In this intermediate- to advanced-level class you'll learn the art of exploiting Web applications so you can find flaws in your enterprise's Web apps before the bad guys do. Through detailed, hands-on exercises and training from a seasoned professional, you will be taught the four-step process for Web application penetration testing. You will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. You will utilize Cross-Site Scripting attacks to dominate a target infrastructure in our unique hands-on laboratory environment. And, you will explore various other Web app vulnerabilities, in depth, with tried-and-true techniques to finding them, using a structured testing regimen. You will learn the tools and methods of the attacker, so that you can be a powerful defender.

On day one, we will study the attacker's view of the Web, We will learn an attack methodology and how the pen-tester uses JavaScript within the test. On day two, we will study the art of reconnaissance, specifically targeted to Web applications. We will also examine the mapping phase as we interact with a real application to determine its internal structure. During day three, we will continue our test by starting the discovery phase using the information we gathered on day two. We will focus on application/server-side discovery. On day four, we will continue discovery, focusing on client-side portions of the application, such as Flash objects and Java applets. On day five, we will move into the final stage of exploitation. Students will use advanced exploitation methods to gain further access within the application. Day six will be a Capture the Flag event where the students will be able to use the methodology and techniques explored during class to find and exploit the vulnerabilities within an intranet site.

Throughout the class, you will learn the context behind the attacks so that you intuitively understand the real-life applications of our exploitation. In the end, you will be able to assess your own organization's Web applications to find some of the most common and damaging Web application vulnerabilities today.

Who Should Attend

- General security practitioners
- Web site designers and architects
- Developers

Get GWAPT Certified

Reinforce what you learned in training and prove your skills and knowledge with a GWAPT certification.
www.giac.org

"Great material and applicable techniques."
-Dennis Dragos, New York City Police Department

"Course was very beneficial. The topics were pertinent and very well thought out."
-Anonymous

Tanya Baccam *Senior Instructor*

Tanya is a senior SANS instructor as well as a SANS courseware author. She also provides many security consulting services, such as system audits, vulnerability and risk assessments, database assessments, Web application assessments, and penetration testing. She has previously worked as the director of assurance services for a security services consulting firm, as well as manager of infrastructure security for a healthcare organization. She also served as a manager at Deloitte & Touche in the Security Services practice. Throughout her career she has consulted with many clients about their security architecture, including areas such as perimeter security, network infrastructure design, system audits, Web server security, and database security. She has played an integral role in developing multiple business applications and currently holds the CPA, GCFW, GCIH, CISSP, CISM, CISA, CCNA, CCSE, CCSA, and Oracle DBA certifications.

SECURITY 566

Implementing and Auditing the Twenty Critical Security Controls - In Depth

Five-Day Program • Mon, August 2 - Fri, August 6, 2010 • 9:00am - 5:00pm
30 CPE Credits • Laptop Required • Instructor: Dr. Eric Cole

Who Should Attend

- Information assurance auditors
- System implementers/ administrators
- Network security engineers
- IT administrators
- DoD personnel/contractors
- Federal agencies/clients
- Private sector organizations looking for information assurance priorities for securing their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD 440, SEC401, SEC501, SANS Audit classes, and MGT512

This course helps you master specific, proven techniques and tools needed to implement and audit the Top Twenty Most Critical Security Controls.

These Top 20 Security Controls, listed below, are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the US military and other government and private organizations (including NSA, DHS, GAO, and many others) who are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block the known attacks and the best way to help find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network through effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Top 20 controls are effectively implemented. It closely reflects the Top 20 Critical Security Controls found at **http://www.sans.org/critical-security-controls**.

One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you'll be stopping or mitigating. That makes the defenses very real, and it makes you a better security person.

Top 20 Critical Security Controls

Critical Controls Subject to Automated Collection, Measurement, and Validation:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations of Network Devices Such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based On Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention

Additional Critical Controls (not directly supported by automated measurement and validation):

16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Training to Fill Gaps

Eric Cole, PhD *SANS Faculty Fellow*

Dr. Eric Cole is an industry-recognized security expert with over 15 years of hands-on experience. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. Cole has a master's degree in computer science from NYIT and a PhD from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is also the CTO of the Americas for McAfee. Cole is actively involved with the SANS Technology Institute (STI) and SANS working with students, teaching, and maintaining and developing courseware. He is a SANS faculty fellow and course author.

Register at www.sans.org/boston-2010

Computer Forensic Essentials

FORENSICS 408

http://forensics.sans.org

Five-Day Program • Mon, August 2 - Fri, August 6, 2010 • 9:00am - 5:00pm
30 CPE Credits • Laptop Required • Instructor: Chad Tilbury

Master computer forensics. Learn essential investigation techniques.

With today's ever-changing technologies and environments, it is inevitable that organizations will deal with some form of cybercrime. These forms include, but are not exclusive to, fraud, insider threat, industrial espionage, and phishing. In order to help solve these cases, organizations are hiring digital forensic professionals and calling cybercrime law enforcement agents to fight and solve these cyber crimes.

FOR408 focuses on the essentials that a forensic investigator must know to investigate core computer crime incidents successfully. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

This course covers the fundamental steps of the in-depth computer forensic methodology so that each student will have the complete qualifications to work as a computer forensic investigator in the field helping solve and fight crime.

This course is the first course in the SANS Computer Forensic Curriculum. If this is your first computer forensics course, we recommend that you start here.

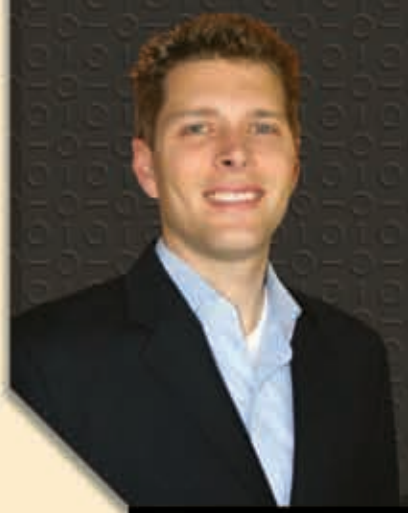
FIGHT CRIME. UNRAVEL INCIDENTS...ONE BYTE AT A TIME.

As a part of this course you will receive a SANS Investigative Forensic Toolkit (SIFT) Essentials with a Tableau Write Block Acquisition Kit. The entire kit will enable each investigator to accomplish proper and secure examinations of SATA, IDE, or Solid State Drives (SSD). The toolkit consists of:

- **Tableau T35e Write Blocker Kit**
  - **One Tableau T35e Write Blocker (Read-Only)**
  - **IDE Cable/Adapters**
  - **SATA Cable/Adapters**
  - **FireWire and USB Cable Adapters**
  - **Forensic Notebook Adapters (IDE/SATA)**
  - **HELIX Incident Response & Computer Forensics Live CD**
- **SANS Windows XP Forensic Analysis VMware Workstation**
- **Course DVD: Loaded with case examples, tools, and documentation**

Who Should Attend

- Information technology professionals interested in the core concepts in computer forensics investigations and e-discovery
- Law enforcement officers, federal agents, or detectives who desire to be introduced to core forensic techniques and topics
- Information security managers who need to understand digital forensics for the information security implications and potential litigation related issues or manage investigative teams
- Information technology lawyers and paralegals who need to understand the basics of digital forensic investigations
- Anyone interested in computer forensic investigations with some background in information systems, information security, and computers



Chad Tilbury *Certified Instructor*

Chad Tilbury has spent over ten years conducting incident response and forensic investigations. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a special agent with the Air Force Office of Special Investigations, he investigated a variety of computer crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and more recently as the vice president of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over sixty countries. Chad is a graduate of the U.S. Air Force Academy and holds a BS and MS in computer science as well as GCFA, GCIH, and CISSP certifications. He is currently a consultant specializing in incident response, e-discovery, and computer forensics.

SANS Computer Forensic Website

forensics.sans.org

The learning does not end when class is over. SANS Computer Forensic Website is a community-focused site offering digital forensics professionals a one-stop forensic resource where they can learn, discuss, and share current developments in the field.

POST-EVENT SKILL-BASED SHORT COURSES

MGT305: Technical Communication and Presentation Skills for Security Professionals

One-Day Course • Sun, August 8, 2010 • 9:00am - 5:00pm • 6 CPE Credits
Laptop Recommended • Instructor: David Hoelzer

This course is designed for every IT professional in your organization. In this course we cover the top techniques that will show any attendee how to research and write professional quality reports, how to create outstanding presentation materials, and as an added bonus, how to write expert witness reports. Attendees will also get a crash course on advanced public speaking skills.

MGT421: SANS Leadership and Management Competencies

One-Day Course • Sat, August 7, 2010 • 9:00am - 5:00pm • 6 CPE Credits
Laptop Recommended • Instructor: Stephen Northcutt

Leadership is a capability that must be learned and developed to better ensure organizational success. Our focus is purely leadership-centric – we are not security-centric or technology-centric with this training opportunity. We help an individual develop leadership skills that apply to commercial business, non-profit, not-for-profit, or other organization. This course is designed to develop existing and new supervisors and managers who aspire to go beyond being the boss and build leadership skills to enhance their organizational climate through team-building to enhance the organizational mission through growth in productivity, workplace attitude / satisfaction, and staff and customer relationships.

SEC517: Cutting-Edge Hacking Techniques

One-Day Course • Sun, August 8, 2010 • 9:00am - 5:00pm • 6 CPE Credits
Laptop Recommended • Instructor: John Strand

Computer attackers continue their relentless march in improving their tools and techniques. The simple scanning of yesteryear has given way to powerful suites of bundled, automated scanning and exploitation tools. Straightforward backdoors have evolved into powerful kernel-mode Root-Kits, manipulating the very hearts of our systems. Covert channels exfiltrate sensitive information and hash collision attacks are rapidly advancing, with your systems in the cross hairs. In all of these trends, thorough reconnaissance and deep subterfuge dominate the attackers' game.

If we don't keep up with their latest methods, our overall defenses and incident response practices will grow rusty. To help fight back, this action-packed, one-day course describes these latest attack trends and what you can do to thwart the bad guys. In addition to detailed descriptions of how the attacks function, you'll get hands-on experience with the tools and their defenses.

Deep discounts are available when these course are taken with a five- or six-day course.

SANS @Night

Evening talks given by our faculty and selected subject matter experts help you broaden your knowledge, get the most for your training dollar, and hear from the voices that matter in computer security.

Community Of Interest in Networking and Security (COINS) Vendor reception

Speaker: Stephen Northcutt

Rapid Response Security Strategy Competition (RRSSC)

Do you know security? Questions from the various security disciplines will be asked in open session: raise your flag to answer; if you are right, you gain a point; if you are wrong, you lose one.

Shabu Zen White T-shirt Contest

Visit www.sans.org/boston-2010/special.php for more information.

Registration Information

We recommend you register early to ensure you get your first choice of courses.
To register, go to www.sans.org/boston-2010

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**6/23/10**	**$400.00**	**7/7/10**	**$250.00**

Group Savings (Applies to tuition only)

15% discount if 12 or more people from the same organization register at the same time
10% discount if 8–11 people from the same organization register at the same time
5% discount if 4–7 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at www.sans.org/conference/discount.php prior to registering.

To register, go to www.sans.org/boston-2010

Select your course or courses and indicate whether you plan to test for GIAC certification.

How to tell if there is room available in a course:
If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

SANS Voucher Credit Program

Expand your Training Budget! Extend your Fiscal Year. The SANS Discount Program that pays you credits and delivers flexibility

www.sans.org/vouchers

Look for E-mail Confirmation – It Will Arrive Soon After You Register

We recommend you register and pay early to ensure you get your first choice of courses. An immediate e-mail confirmation is sent to you when the registration is submitted properly. If you have not received e-mail confirmation within two business days of registering, please call the SANS Registration office at 301-654-7267 9:00am - 8:00pm Eastern Time.

Cancellation

You may substitute another person in your place at any time by e-mail: registration@sans.org or faxing to 301-951-0140. There is a $300 cancellation fee per registration. Cancellation requests must be received by **Wednesday, July 14, 2010** by fax or mail-in order to receive a refund.

Hotel Information

Conference Location

Hyatt Regency Boston
One Avenue de Lafayette
Boston, Massachusetts 02111
Tel: 617-912-1234 • Fax: 617-451-2198
Website: http://regencyboston.hyatt.com

A special discount rate of $194 S/D will be honored based on space availability. This rate includes high-speed Internet in your room. Make your reservations now as this special rate is only available through July 11, 2010. To make reservations, please call 1-800-233-1234.

Note: You must mention that you are attending the SANS Institute training to get the discounted rate.

Top 5 reasons to stay at the Hyatt Regency Boston:

1. **All SANS attendees receive complimentary high-speed Internet when booking in the SANS Block.**
2. **No need to factor in daily cab fees and the time associated with travel to alternate hotels.**
3. **By staying at the Hyatt Regency Boston, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the conference.**
4. **SANS schedules morning and evening events at the Hyatt Regency Boston that you won't want to miss!**
5. **Everything is in one convenient location!**

Future SANS Training Events

SANSFIRE 2010
June 6 - 14, 2010 • Baltimore, MD

SANS Rocky Mountain 2010
July 12 - 17, 2010 • Denver, CO

SANS Boston 2010
August 2 - 8, 2010 • Boston, MA

SANS Portland 2010
August 23 - 28, 2010 • Portland, OR

SANS Virginia Beach 2010
August 27 - September 3, 2010 • Virginia Beach, VA

SANS Network Security 2010
September 19 - 27, 2010 • Las Vegas, NV

SANS Chicago 2010
October 25 - 31, 2010 • Skokie, IL

SANS San Antonio 2010
November 13 - 20, 2010 • San Antonio, TX

SANS CDI 2010
December 10 - 16, 2010 • Washington, DC

For a full list of training events, please visit www.sans.org.
Dates and locations are subject to change.

SANS 8120 Woodmont Avenue
Suite 205
Bethesda, MD 20814

Save $400 when you register by June 23rd
www.sans.org/boston-2010

Use this promo code when you register.