“Wow. This is the BEST training I have EVER encountered.”
—Stanley de Jager, Symantec
SANS Online Training includes four formats that allow you to choose the workflow, interaction and speed of training that you prefer.

Whether you choose to use OnDemand, vLive, Simulcast or SelfStudy to complete your SANS training online, the benefits of SANS online training always include:

- No Travel: Train from anywhere in the world
- Instruction from SANS’ top instructors
- Online access to your course materials, labs and instructor lectures
- All of the same printed course materials as live courses
- Subject-Matter Expert support to assist you with course content

You can also bundle the benefits of OnDemand training with any live SANS course.

Learn more about all of the online training options available from SANS by visiting www.sans.org/online-security-training.

For more detailed information about our Online Training formats, turn to pages 2-7.

“I hold three GIAC certifications, have attended multiple classes, and nothing prepares me to do my job better than SANS Online Training.” —Rick Whitmore, University of Kansas

SANS Institute is the most trusted and largest provider of live training (from small groups to multi-course training events), online training (from self-paced to instructor-led), certification, education and free community resources to information security professionals around the world.

This training guide and the enclosed IT Security Training Roadmap will help you to plan your education and accelerate your career! The roadmap pullout contains all of the course, certification and career information you need to chart a course to success in Cyber Defense, Penetration Testing, Digital Forensics and Incident Response, or another information security field. Find the roadmap between pages 10 and 11.

Also in this catalog: Pages
SANS Upcoming Live Events 11
Cyber Defense 14 - 15
Penetration Testing 16 - 17
Digital Forensics 18 - 19
Additional SANS Courses 20
OnDemand

Train Anytime, Anywhere, At Your Own Pace

If you’re a self-motivated learner who prefers a flexible training schedule, then SANS OnDemand is the right learning platform for you. Choose from more than 30 courses, and take them whenever and wherever you want.

Each course gives you four months of access to our OnDemand computer-based training platform, which includes a mix of presentation slides, video demonstrations, quizzes, and audio of SANS’ top instructors teaching the material. If you have questions about the material, our subject-matter experts are available to help.

You can also bundle OnDemand with any other SANS online or in-person training vehicles to diversify your learning experience or bolster your preparation for the GIAC certification exam.

For more information, contact us:
ondemand@sans.org
301-654-SANS (7267)
sans.org/ondemand

“I love the OnDemand option. With family and work schedules, OnDemand was the only way I could finish the course. I also really enjoyed listening to the class.”
—Fred Leezer, Cardinal Health

Reasons to Choose SANS OnDemand

- Four Months of Access to Comprehensive Online Training and Quizzes
- Web-Based Training Accessible 24/7 From Your Desktop, Laptop, iPad, or Android Tablet
- Taught by SANS’ Top Gun Instructors, Including Dr. Eric Cole, Rob Lee, and Ed Skoudis
- No Travel or Time Away From the Office
- Includes Video Labs and Hands-On Exercises
- Access to Highly-Qualified Subject-Matter Experts
- Complete Set of Course Books and Hands-On CDs
- Course Progress Reports
- Over 30 Courses Available – Anytime, Anywhere
- Supplemental Preparation Tool for the GIAC Exam

OnDemand Courses

IT Security and Penetration Testing:
- SEC301: Intro to Information Security
- SEC401: Security Essentials Bootcamp Style
- SEC501: Advanced Security Essentials - Enterprise Defender
- SEC502: Perimeter Protection In-Depth
- SEC503: Intrusion Detection In-Depth
- SEC504: Hacker Tools, Techniques, Exploits & Incident Handling
- SEC505: Securing Windows with the Critical Security Controls
- SEC506: Securing Linux/Unix
- SEC511: Continuous Monitoring and Security Operations
- SEC542: Web App Penetration Testing and Ethical Hacking
- SEC560: Network Penetration Testing and Ethical Hacking
- SEC566: Implementing and Auditing the Critical Security Controls - In-Depth
- SEC575: Mobile Device Security and Ethical Hacking
- SEC579: Virtualization and Private Cloud Security
- SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses
- SEC642: Advanced Web App Penetration Testing and Ethical Hacking
- SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Digital Forensics & Incident Response:
- FOR408: Windows Forensic Analysis
- FOR508: Advanced Digital Forensics and Incident Response
- FOR518: Mac Forensic Analysis
- FOR526: Memory Forensics In-Depth
- FOR572: Advanced Network Forensics and Analysis
- FOR585: Advanced Smartphone Forensics
- FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Security Management:
- MGT414: SANS Training Program for CISSP® Certification
- MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™
- MGT514: IT Security Strategic Planning, Policy and Leadership

Software Security:
- DEV522: Defending Web Applications Security Essentials
- DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
- DEV544: Secure Coding in .NET: Developing Defensible Applications

IT Audit:
- AUD507: Auditing & Monitoring Networks, Perimeters & Systems

Legal Security:
- LEG523: Law of Data Security and Investigations

Industrial Control Systems:
- ICS410: ICS/SCADA Security Essentials

For the latest OnDemand courses and online training promotions visit:
www.sans.org/online-security-training/specials
vLive

Live Online Training from Your Own Home or Office

vLive courses from SANS Institute are taken via online classrooms that typically meet twice per week for six weeks and are taught by SANS’ top instructors. They feature challenging labs and exercises that develop skills and reinforce concepts, and are supported by subject-matter experts.

Simply log in at the scheduled times and join your instructor and classmates in an interactive virtual classroom. Don’t worry if you can’t attend every live session; classes are recorded and you can review the class archives for six months.

For more information, contact us:
vlive@sans.org
301-654-SANS (7267)
sans.org/vlive

Reasons to Choose SANS vLive

- Live Evening Courses Taken from the Convenience of Your Home or Office
- Six Months of Online Course Access
- Taught by SANS’ Top Gun Instructors, Including Dr. Eric Cole, Rob Lee and Ed Skoudis
- Meet Twice per Week for Six Weeks
- Course Content Authored by Instructors
- Labs, Hands-On Exercises and Archived Lectures
- Highly-Qualified Subject-Matter Expert Support
- Complete Set of Books and CDs

2016 Course Schedule:

Jan.25 - Mar.2   FOR572: Advanced Network Forensics and Analysis
Feb.2 - Mar.10   SEC11: Continuous Monitoring and Security Operations
Feb.8 - Mar.16   SEC401: Security Essentials Bootcamp Style
Mar.22 - Apr.28  SEC504: Hacker Tools, Techniques, Exploits & Incident Handling
Apr.11 - May 18  SEC360: Network Penetration Testing and Ethical Hacking
Apr.25 - Jun.1   MGT414: SANS Training Program for CISSP® Certification
May 10 - Jun.16  FOR508: Advanced Digital Forensics and Incident Response
Jun.21 - Jul.28   FOR610: Reverse Engineering Malware: Malware Analysis Tools and Techniques
Jun.27 - Aug.3   SEC42: Web App Penetration Testing and Ethical Hacking
Jul.5 - Aug.11   SEC504: Hacker Tools, Techniques, Exploits and Incident Handling
Jul.11 - Aug.10  SEC301: Intro to Information Security
Jul.19 - Aug.25  MGT414: SANS Training Program for CISSP® Certification
Jul.25 - Aug.31  SEC401: Security Essentials Bootcamp Style
Aug.8 - Sep.7    SEC512: SANS Security Leadership Essentials For Managers with Knowledge Compression™
Aug.16 - Sep.22  SEC360: Network Penetration Testing and Ethical Hacking
Sep.19 - Oct.26  SEC303: Intrusion Detection In-Depth
Sep.27 - Nov.3   SEC11: Continuous Monitoring and Security Operations
Oct.11 - Nov.17  FOR408: Windows Forensic Analysis
Oct.17 - Nov.23  FOR508: Advanced Digital Forensics and Incident Response
Nov.1 - Dec.8    SEC504: Hacker Tools, Techniques, Exploits and Incident Handling
Nov.7 - Dec.14   MGT414: SANS Training Program for CISSP® Certification
Nov.15 - Jan.5   FOR572: Advanced Network Forensics and Analysis
Dec.5 - Jan.25   SEC42: Web App Penetration Testing and Ethical Hacking
Dec.6 - Jan.26   SEC360: Network Penetration Testing and Ethical Hacking

“For the latest vLive courses and online training promotions visit: www.sans.org/online-security-training/specials

Course offerings and schedules are subject to change, please visit www.sans.org/online-security-training for regularly updated information.

“Overall, I am much happier with the web-based live training as a) no travel required, b) no travel budget required, and c) some ‘soak time’ between modules (as well as time to complete the exercises before the next session). It’s still a bit of a fire hose to drink from, but I would heartily recommend this format.”

- Bill Stackpole, Rochester Institute of Technology
Simulcast

Attend a SANS Training Event Without Leaving Home

Simulcast training from SANS Institute gives you the opportunity to attend a one-week live training event from your own home or office via distance learning technology. Complete a SANS course quickly from anywhere in the world while still benefiting from real-time interaction with a top SANS instructor and a classroom of peers.

For more information, contact us:
simulcast@sans.org
301-654-SANS (7267)
sans.org/simulcast

“I’m at home taking the online Simulcast class but I feel like I’m there in the room. I don’t feel isolated at all. I just have access to my comforts while taking the class.”

- Deona Vastine, State of California

Reasons to Choose SANS Simulcast

- Live Daytime Courses Taken from the Convenience of Your Home or Office
- Four Months of Online Course Access
- Taught by SANS’ Top Gun Instructors, Including Dr. Eric Cole, Rob Lee and Ed Skoudis
- Complete a Course in One Week
- Course Content Authored by Instructors
- Labs, Hands-On Exercises and Archived Lectures
- Highly-Qualified Subject-Matter Expert Support
- Complete Set of Books and CDs
- No Travel Required

2016 Simulcast Schedule

Live from SANS Anaheim 2016
Feb. 22 - 26  SEC301: Intro to Information Security
Feb. 22 - 27  SEC401: Security Essentials Bootcamp Style
Feb. 22 - 27  SEC503: Intrusion Detection In-Depth
Feb. 22 - 27  SEC504: Hacker Tools, Techniques, Exploits and Incident Handling
Feb. 22 - 27  FOR508: Advanced Digital Forensics and Incident Response

Live from SANS 2016
Mar. 14 - 19  FOR408: Windows Forensic Analysis
Mar. 14 - 19  SEC511: Continuous Monitoring and Security Operations
Mar. 14 - 19  SEC560: Network Penetration Testing and Ethical Hacking

Live from SANS Pen Test Austin 2016
Apr. 1 - 23  SEC401: Security Essentials Bootcamp Style
Apr. 18 - 23  SEC504: Hacker Tools, Techniques, Exploits and Incident Handling
Apr. 18 - 23  SEC560: Network Penetration Testing and Ethical Hacking
Apr. 18 - 23  SEC642: Advanced Web App Penetration Testing and Ethical Hacking
Apr. 18 - 23  SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Live from SANS Houston 2016
May 9 - 14  SEC401: Security Essentials Bootcamp Style
May 9 - 14  SEC503: Intrusion Detection In-Depth
May 9 - 14  SEC504: Hacker Tools, Techniques, Exploits and Incident Handling
May 9 - 14  SEC511: Continuous Monitoring and Security Operations
May 9 - 14  SEC560: Network Penetration Testing and Ethical Hacking

Live from SANSFIRE 2016
Jun. 13 - 18  FOR408: Windows Forensic Analysis
Jun. 13 - 18  FOR508: Advanced Digital Forensics and Incident Response
Jun. 13 - 18  FOR518: Mac Forensic Analysis
Jun. 13 - 18  SEC560: Network Penetration Testing and Ethical Hacking
Jun. 13 - 18  FOR572: Advanced Network Forensics and Analysis
Jun. 13 - 18  SEC504: Hacker Tools, Techniques, Exploits and Incident Handling

Live from SANS Chicago 2016
Aug. 22-27  SEC504: Hacker Tools, Techniques, Exploits and Incident Handling
Aug. 22-27  FOR508: Advanced Digital Forensics and Incident Response
Aug. 22-27  SEC511: Continuous Monitoring and Security Operations
Aug. 22-26  LEG523: Law of Data Security and Investigations

Course offerings are subject to change, please visit
www.sans.org/online-security-training for regularly updated information.
SelfStudy

Self-paced training for the motivated and disciplined student.

IT Security
- SEC301: Intro to Information Security
- SEC401: Security Essentials Bootcamp Style
- SEC440: Critical Security Controls: Planning, Implementing and Auditing
- SEC501: Advanced Security Essentials - Enterprise Defender
- SEC502: Perimeter Protection In-Depth
- SEC503: Intrusion Detection In-Depth
- SEC505: Securing Windows with the Critical Security Controls
- SEC506: Securing Linux/Unix
- SEC511: Continuous Monitoring and Security Operations
- SEC524: Cloud Security Fundamentals
- SEC546: IPv6 Essentials
- SEC566: Implementing and Auditing the Critical Security Controls - In-Depth
- SEC579: Virtualization and Private Cloud Security
- SEC580: Metasploit Kung Fu for Enterprise Pen Testing

Penetration Testing:
- SEC504: Hacker Techniques, Exploits & Incident Handling
- SEC542: Web App Penetration Testing and Ethical Hacking
- SEC560: Network Penetration Testing and Ethical Hacking
- SEC575: Mobile Device Security and Ethical Hacking
- SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses
- SEC642: Advanced Web App Penetration Testing and Ethical Hacking
- SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Digital Forensics & Incident Response:
- FOR408: Windows Forensic Analysis
- FOR508: Advanced Digital Forensics and Incident Response
- FOR518: Mac Forensic Analysis
- FOR526: Memory Forensics In-Depth
- FOR572: Advanced Network Forensics and Analysis
- FOR585: Advanced Smartphone Forensics
- FOR601: Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Security Management:
- MGT405: Technical Communication and Presentation Skills for Security Professionals
- MGT414: SANS® Training Program for CISSP® Certification
- MGT415: A Practical Introduction to Cyber Security Risk Management
- MGT432: SANS Security Leadership Essentials for Managers with Knowledge Compression™
- MGT514: IT Security Strategic Planning, Policy and Leadership
- MGT535: Incident Response Team Management

Software Security:
- DEV522: Defending Web Applications Security Essentials
- DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
- DEV544: Secure Coding in .NET: Developing Defensible Applications

IT Audit:
- AUD507: Auditing & Monitoring Networks, Perimeters & Systems

Legal Security:
- LEG523: Law of Data Security and Investigations

Industrial Control Systems:
- ICS410: ICS/SCADA Security Essentials

Build a Private Simulcast for Your Organization

SANS has the ability to build a custom Private Simulcast to meet your organization's specific distributed workforce training needs. We will send an instructor, as well as courseware and toolkits for every student, and Simulcast the training as needed to deliver a SANS course in any curriculum to your local or global workforce or group.

For more information about this Private Simulcast training opportunity, visit www.sans.org/private-training/online.

Online Training Voucher Program

SANS offers a Voucher Credit purchasing program that can be utilized to get more information security training from your budget for a multi-student group. Bonus credits are available to those organizations that choose to use Online Training only for their group training, and those credits can be used to register for any OnDemand or vLive course, and for GIAC certification attempts and exams.

For more information about the SANS Voucher Program, visit www.sans.org/vouchers.
SANS Institute is a respected world leader in providing knowledge and training to information security professionals. Since 1989, we’ve developed a full range of training and tools through which professionals can gain vital experience and education.

In addition, we also have programs and resources such as Private custom training options, free webcasts, blogs and papers, the Cyber Talent applicant assessment program, and the annual “Difference Maker” Awards. Learn more about SANS Institute anytime, at:

www.sans.org

Live and Online Training
Courses are taught around the world or via online access by an unparalleled faculty of industry leaders.
www.sans.org

SANS Technology Institute
Accredited Graduate Programs and Graduate Certificates in Information Security completed via SANS training.
www.sans.edu

GIAC
More than 27 specialized cyber security certifications are offered, including Cyber Defense, Penetration Testing, Digital Forensics, Management and more.
www.giac.org

Securing The Human
Employee Security Awareness program applicable to every organization.
www.securingthehuman.org

Internet Storm Center
Moment-by-moment intrusion detection news for the world’s cyber defense community.
isc.sans.edu

NetWars
A suite of hands-on, interactive scenario challenges to help students master a wide range of skills.
www.sans.org/netwars

Where to find the SANS Institute:

Facebook: SANS Institute
Twitter: @SANSInstitute
LinkedIn: SANS Institute
RSS Feeds: www.sans.org/rss.php
Blogs: www.sans.org/security-resources/blogs
Webcasts: www.sans.org/webcasts
Internet Storm Center: isc.sans.edu
SANS Reading Room: www.sans.org/reading-room

Upcoming Live Events

SANS Las Vegas 2016
Las Vegas, NV • January 9-14 2016
www.sans.org/event/las-vegas-2016

SANS Security East 2016
New Orleans, LA • January 25-30 2016
www.sans.org/event/security-east-2016

SANS Scottsdale 2016
Scottsdale, AZ • February 8-13, 2016
www.sans.org/event/scottsdale-2016

SANS McLean 2016
McLean, VA • February 15-20, 2016
www.sans.org/event/mclean-2016

SANS Anaheim 2016
Anaheim, CA • February 22-27, 2016
www.sans.org/event/anaheim-2016

SANS 2016
Orlando, FL • March 12-19, 2016
www.sans.org/event/sans-2016

30+ Courses Available!
Graduate Programs in Information Security

The accredited Master of Science degrees in Information Security from SANS Technology Institute are the mark of a cybersecurity professional with deep technical and organizational capabilities.

Both the Master of Science in Information Security Engineering and the Master of Science in Information Security Management will help you to demonstrate your advanced skills in leading the information security efforts for your organization.

Shorter course programs are also available to earn topic-specific certificates.

Visit www.sans.edu today to learn more about the benefits of earning degrees or certificates from the SANS Technology Institute.

NetWars Continuous

Embrace the Challenge

SANS’ NetWars Continuous Online Range uses the gamification of IT Security to advance your most vital InfoSec skills.

To build your skills and keep them from getting rusty, you need an environment where you can apply your knowledge to solving real-world, real-time infosec issues to stay sharp. That’s what NetWars Continuous is all about. Over the course of 4 months and 5 levels, you can master real-world tactics and techniques in a safe learning environment.

Fully executed online, NetWars Continuous includes automated hints and support from the SANS NetWars team to ensure that you have the most rewarding experience possible. The challenge also delivers twice as many CPE credits (12) as a live NetWars Tournament (6), and can be completed by participants at any level of experience, so there is no reason for anyone to be intimidated by NetWars.

Begin your online NetWars journey now at www.sans.org/netwars/continuous.

GIAC tests and validates the ability of practitioners in information security, forensics, and software security. GIAC Certification holders possess comprehensive cyber security skills to protect critical IT infrastructure, and are sought after globally by government, military and industry to protect the cyber environment.

More than 30 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, IT security law, and industrial control systems are available now. Learn more about pursuing your GIAC Certification at www.giac.org.

“GIAC defines a higher level of mastery and skill that is required in order to earn the credential. GIAC really stands out among other security certifications.”
- Josh Ringer, Benfis Health System
The five-step Cyber Defense process outlined below will enable you to identify risk, determine highest priorities, focus in on the areas that really matter, and measure progress against established baselines to improve overall security posture.

Five Key Steps to Cyber Defense

**Step 1: Identify Critical Data**
Align critical assets with threats and vulnerabilities to focus on risk
1. What is the risk? 2. Is it the highest-priority risk? 3. What is the most cost-effective way of reducing the risk?

**Step 2: Align the Defense with the Offense**
If the defense knows more than the offense, you will lose
Requirements: 1. Accurate up-to-date network diagram 2. Network visibility map 3. Configuration management and change control

**Step 3: Know Thy Organization**
If the offense knows more than the defense, you will lose

**Step 4: Defense In-Depth**
There is no such thing as an unstoppable adversary
Requirements: 1. Network security knowledge 2. Network visibility map 3. Configuration management and change control

**Step 5: Common Metrics**
Utilize the Critical Controls
1. Minimize the size of the attack surface
2. Change control and configuration management
3. Metrics to drive measurement and compliance

Cyber Defense Curriculum:

SEC501: Intro to Information Security — This introductory course is the fastest way to get up to speed in information security. The entry-level course includes a broad spectrum of security topics and real-life examples, and can be used to prepare for GISP Certification.

SEC501: Security Essentials Bootcamp Style — In this course, students learn the language and underlying theory of computer and information security. Since all jobs today require an understanding of security, this course will help you understand how security applies to your job. In addition, students will gain the essential and latest knowledge and skills required for effective management of security systems and processes.

SEC501: Advanced Security Essentials - Enterprise Defender — A key theme of this course is that prevention is ideal, but detection is a must. Security professionals must know how to constantly advance security efforts in order to prevent as many attacks as possible. This prevention needs to occur both externally and internally via portable, network and server environments.

SEC502: Perimeter Protection In-Depth— This course is a comprehensive analysis of a wide breadth of protection technologies. As one of the most diverse courses in the SANS catalog, this training gives students a valuable grasp on important information security processes, which they can use to implement many tools.

SEC503: Intrusion Detection In-Depth — The purpose of this course is to acquaint students with the core knowledge, tools and techniques necessary to defend networks. Spanning a wide variety of topics, from foundational materials such as TCP/IP to detecting an intrusion, this training will provide students with in-depth knowledge on intrusion detection.

SEC505: Securing Windows with PowerShell and the Critical Security Controls — In SEC505 students learn to defend against pass-the-hash attacks, administrator account compromise, and the lateral movement of hackers inside the network by implementing the Critical Security Controls and PowerShell in a Windows environment.

SEC506: Securing Linux/Unix — Experience in-depth coverage of Linux and Unix security issues and examine how to mitigate or eliminate general problems that apply to all Unix-like operating systems. Specific configuration guidance and practical, real-world examples, tips, and tricks are provided to help students remove vulnerabilities.

SEC511: Continuous Monitoring and Security Operations — The Defensible Security Architecture and Network Security Monitoring/Continuous Diagnostics and Mitigation/Continuous Security Monitoring taught in this course will best position your organization or Security Operations Center to analyze threats and detect anomalies that could indicate cybercriminal behavior.

SEC566: Implementing and Auditing the Critical Security Controls — In Depth — As threats evolve, an organization’s security should as well. To enable your organization to stay on top of this ever-changing scenario, SANS designed this course to train students how to implement the Twenty Critical Security Controls — a prioritized, risk-based approach to security that was designed by a master group of private- and public-sector experts from around the world.

SEC579: Virtualization and Private Cloud Security
Learn best practices for configuring and designing virtual security controls and infrastructure, and about how your vulnerability assessment and forensic processes can be updated to more accurately detect and manage risks in virtual and cloud environments.
What Makes SANS Penetration Testing Courses Special?

SANS Penetration Testing courses are uniquely crafted to equip students with the methodology and hands-on, offensive techniques that all information security professionals should have to understand their organization’s vulnerabilities to potential adversaries. The courses offered cover a wide variety of technological landscapes that security professionals face, with an in-depth focus on network, web application, mobile device and wireless penetration tests and vulnerability assessments. For the professional penetration tester, our advanced courses offer the latest in exploit development and ethical hacking to help them deliver technical excellence and exemplary business value to their organizations via high-level penetration tests.

What Is High-Value Penetration Testing and Why Is It Important?

A high-value penetration test has several aspects:
• It models the activities of real-world attackers…
• To find vulnerabilities in target systems…
• And exploits them under controlled circumstances…
• Applying technical excellence to determine and document risk and potential business impact…
• In a professional, safe fashion according to a carefully designed scope and rules of engagement…
• With the goal of helping an organization prioritize its resources in improving its security stance!

Penetration Testing Resources
pen-testing.sans.org/resources

Twitter @SANSPenTest
Blog pen-testing.sans.org/blog
Webcasts pen-testing.sans.org/resources/webcasts
GPWN Mailing List lists.sans.org/mailman/listinfo/gpwn-list

“Excellent classroom material and real-world examples are used to enhance understanding of concepts. And the online format allows you to replay content for greater understanding of concepts.” - Curt Lengfelder, PACCAR Inc.

Penetration Testing Curriculum:

SEC504: Hacker Tools, Techniques, Exploits & Incident Handling—Intense attack techniques and their associated defenses are covered in this course, so that offense can inform defense to improve the state of security in your organization by preparing you to handle incidents caused by the latest threats.

SEC542: Web App Penetration Testing and Ethical Hacking—Through detailed, hands-on exercises, this intermediate to advanced level course will provide you with the skills needed to perform web app vulnerability discovery and exploitation for your organization.

SEC560: Network Penetration Testing and Ethical Hacking—In-depth penetration testing skills learned in this course will prepare you to conduct professional-grade pen tests, end-to-end, including scoping, recon, scanning, exploitation, post-exploitation and more.

SEC575: Mobile Device Security and Ethical Hacking—Secure design, deployment, operation and pen testing of mobile devices and their associated infrastructures are the topics of this course. Top-notch lessons on device analysis, app exploitation, mobile device management and wireless infrastructures are included.

SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses—This course is dedicated to the art of analyzing wireless protocols, devices and infrastructures to find vulnerabilities and fix them, with topics ranging from wireless LANs to Bluetooth to ZigBee and more.

SEC642: Advanced Web App Penetration Testing and Ethical Hacking—In this course you will experience intense web app and web services exploitation, diving deep into the mechanics of web app infrastructures and protocols to find and fix subtle yet hugely damaging flaws before the hackers do.

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking—In this course you will experience intense web app and web services exploitation, diving deep into the mechanics of web app infrastructures and protocols to find and fix subtle yet hugely damaging flaws before the hackers do.

Industrial Control Systems Curriculum:

IC410: ICS/SCADA Security Essentials—SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. IC410 ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.
Every organization will eventually deal with cyber crime. Fraud, intrusion, insider threat, phishing and other cyber crimes are now a fact of life. If you are an IT or law enforcement professional and don’t know how to look for and sort out these cases, your skills are becoming less valuable every day.

SANS developed the Digital Forensics and Incident Response courses to train sophisticated incident responders and forensics investigators. A properly trained incident responder could be the only defense your organization has during a compromise. As a forensics investigator, you need to know what you are up against, and you need to have the most up-to-date knowledge of how to detect and fight it – that is what SANS courses will teach you.

Why Is Computer Forensics Important?

Proper handling of a forensics investigation is key to fighting back against computer crimes. A thorough understanding of many areas is required for a proper investigation, including: situation; acquisition; analysis; reporting; presenting; and certification.

- **Situation**
  Incident response teams need to respond to intrusions in addition to e-discovery requests.

- **Acquisition**
  Forensics analysts need to gather digital evidence using approved legal and technical methodologies.

- **Analysis**
  Forensics analysts need to examine data, extracting key evidence while preserving data integrity.

- **Reporting**
  Forensics analysts need to communicate key information to management.

- **Presenting**
  Analysts need to be prepared to present evidence in civil or criminal courts.

- **Certification**
  Forensic certification increases an analyst’s stature in a court of law.

### Forensics Resources:
- Web: digital-forensics.sans.org/community/links
- Blog: digital-forensics.sans.org/blog
- Twitter: @sansforensics
- Facebook: SANSForensics
- Google+: gplus.to/sansforensics
- SIFT Workstation: dfir.to/SANS-SIFT

---

*I am a huge SANS fan, this is my second course and I plan on taking as many as I can fit into the company’s training budget for future years.* - Kurt Manke, Organic Valley
DEVS52: Defending Web Applications Security Essentials — This is the course to take to learn how to defend web applications. Traditional network defenses, such as firewalls, fail to secure web applications. The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure that data.

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications — This course teaches students how to build secure Java applications and gain the knowledge and skills to keep a website from getting hacked. Counter a wide range of attack tactics, prevent critical security vulnerabilities that can lead to data loss, and understand the mindset of attackers. Learn foundational defensive techniques, cutting-edge protection, and Java EE security features you can use in your applications as soon as you return to work.

DEV544: Secure Coding in .NET: Developing Defensible Applications — This course will help students leverage built-in and custom defensive technologies to integrate security into their applications. Students will examine actual code, work with real tools, build applications, and gain confidence in the resources they need to improve the security of .NET applications.

Audit Curriculum:

AUDS07: Auditing & Monitoring Networks, Perimeters & Systems — This course is designed to empower advancing managers to effectively manage and secure the infrastructures of their organizations. The course focuses on the eight domains of knowledge as determined by (ISC)². You will learn to provide a risk-driven method for tackling the enormous task of designing an enterprise security-validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical details and to determine the key controls that can be used to provide a level of assurance to an organization.

Management Curriculum:

MGT514: SANS Training Program for CISSP® Certification — This course is designed to prepare you to pass the current CISSP® Certification Exam. It is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the eight domains of knowledge as determined by (ISC)².

MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™ — 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 will not just learn about security; you will learn how to manage security.

MGT514: IT Security Strategic Planning, Policy and Leadership — This course teaches security professionals how to navigate the ever-growing world of security by developing strategic plans, creating effective information security policy, and developing management and leadership skills.

Legal Curriculum:

LEG523: Law of Data Security and Investigations — This course will teach you the law of business, contracts, fraud, crime, IT security, IT liability and IT policy— all with a focus on electronically stored and transmitted records. The course also teaches investigators how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resources or other investigations.
Don’t miss an opportunity to take SANS Institute’s information security training ever again.

Use our online training formats - OnDemand, vLive, Simulcast or SelfStudy - to train from anywhere in the world, when you prefer and without any travel costs!

Online course specials also make training more feasible. Visit www.sans.org/online-security-training/specials now to see the current special.
The 4 Coolest Jobs in Information Security

**SEC511: Continuous Monitoring and Security Operations**
- Why It’s Cool: Being on the front line, watching attacks and being able to keep an organization’s most critical assets protected and secure. The SOC Analyst is responsible for assessing and monitoring the security risk, the pen tester provides crucial insights into the most pressing issues and suggests how to prioritize security resources. This expert finds security vulnerabilities in target systems, networks, and applications, using tools and techniques to test the strength of safeguards and identify potential weaknesses. Why It’s Cool: SOC Analysts are the eyes and ears of the organization, providing real-time monitoring of the network and alerting security personnel to potential threats. They help you master a subject in all of its depth and complexity.

**SEC502: Perimeter Protection In-Depth**
- Why It’s Cool: The SOC Analyst is responsible for assessing and monitoring the security risk, the pen tester provides crucial insights into the most pressing issues and suggests how to prioritize security resources. This expert finds security vulnerabilities in target systems, networks, and applications, using tools and techniques to test the strength of safeguards and identify potential weaknesses. Why It’s Cool: SOC Analysts are the eyes and ears of the organization, providing real-time monitoring of the network and alerting security personnel to potential threats. They help you master a subject in all of its depth and complexity.

**SEC503: Intrusion Detection In-Depth**
- Why It’s Cool: The SOC Analyst is responsible for assessing and monitoring the security risk, the pen tester provides crucial insights into the most pressing issues and suggests how to prioritize security resources. This expert finds security vulnerabilities in target systems, networks, and applications, using tools and techniques to test the strength of safeguards and identify potential weaknesses. Why It’s Cool: SOC Analysts are the eyes and ears of the organization, providing real-time monitoring of the network and alerting security personnel to potential threats. They help you master a subject in all of its depth and complexity.

**SEC502: Perimeter Protection In-Depth**
- Why It’s Cool: The SOC Analyst is responsible for assessing and monitoring the security risk, the pen tester provides crucial insights into the most pressing issues and suggests how to prioritize security resources. This expert finds security vulnerabilities in target systems, networks, and applications, using tools and techniques to test the strength of safeguards and identify potential weaknesses. Why It’s Cool: SOC Analysts are the eyes and ears of the organization, providing real-time monitoring of the network and alerting security personnel to potential threats. They help you master a subject in all of its depth and complexity.

**SEC502: Perimeter Protection In-Depth**
- Why It’s Cool: The SOC Analyst is responsible for assessing and monitoring the security risk, the pen tester provides crucial insights into the most pressing issues and suggests how to prioritize security resources. This expert finds security vulnerabilities in target systems, networks, and applications, using tools and techniques to test the strength of safeguards and identify potential weaknesses. Why It’s Cool: SOC Analysts are the eyes and ears of the organization, providing real-time monitoring of the network and alerting security personnel to potential threats. They help you master a subject in all of its depth and complexity.
Beginners

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

Many of these courses are also offered at live events! Visit www.sans.org for a complete listing of SANS events.