THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS Charlotte 2017

June 12-17

PROTECT YOUR COMPANY AND ADVANCE YOUR CAREER
WITH HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Five courses in:

CYBER DEFENSE
PENETRATION TESTING
DIGITAL FORENSICS
ETHICAL HACKING
ICS/SCADA SECURITY

"The training was directly on point to the kind of work I am doing and immediately increased my knowledge and skills in these areas."
-JOE MINDOCK, CSG GOVERNMENT SOLUTIONS

GIAC CERTIFICATIONS
GIAC-Approved Training

SAVE $400

Register and pay by April 19th – Use code **EarlyBird17**

www.sans.org/charlotte

SANS Instructors

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS Charlotte 2017 lineup of instructors includes:

Carlos Cajigas
Certified Instructor
@Carlos_Cajigas

Eric Cornelius
Certified Instructor

Mick Douglas
Instructor
@BetterSafetyNet

Jonathan Ham
Certified Instructor
@jhamcorp

Jeff McJunkin
Instructor
@jeffmcjunkin

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 7.

Virtualizing Forensic Images Using Free Tools in Linux
Carlos Cajigas

Becoming a Better Technologist by Becoming Better at Business
Eric Cornelius

Building Your Own Kickass Home Lab
Jeff McJunkin

The training campus for SANS Charlotte 2017, Hilton Charlotte University Place, offers a tranquil lakeside escape near UNC Charlotte and the area's best shopping destinations.

PAGE 13

Save $400 when you register and pay by April 19th using code EarlyBird17

Courses at a Glance

	MON 6-12	TUE 6-13	WED 6-14	THU 6-15	FRI 6-16	SAT 6-17
SEC401 Security Essentials Bootcamp Style	Page 2					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 3					
SEC560 Network Penetration Testing and Ethical Hacking	Page 4					
FOR408 Windows Forensic Analysis	Page 5					
ICS410 ICS/SCADA Security Essentials	Page 6					

SANS Training Formats

Whether you choose to attend a training class live or online, the entire SANS team is dedicated to ensuring your training experience exceeds expectations.

Live Classroom Instruction

Premier Training Events

Our most recommended format, live SANS training events deliver SANS' top instructors teaching multiple courses at a single time and location, allowing

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified Instructors
- Interactions and learning from other professionals
- @Night events, NetWars, Vendor presentations, industry receptions, and many other benefits

Our premier live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year. See page 97 for upcoming Training Events in North America.

Summits

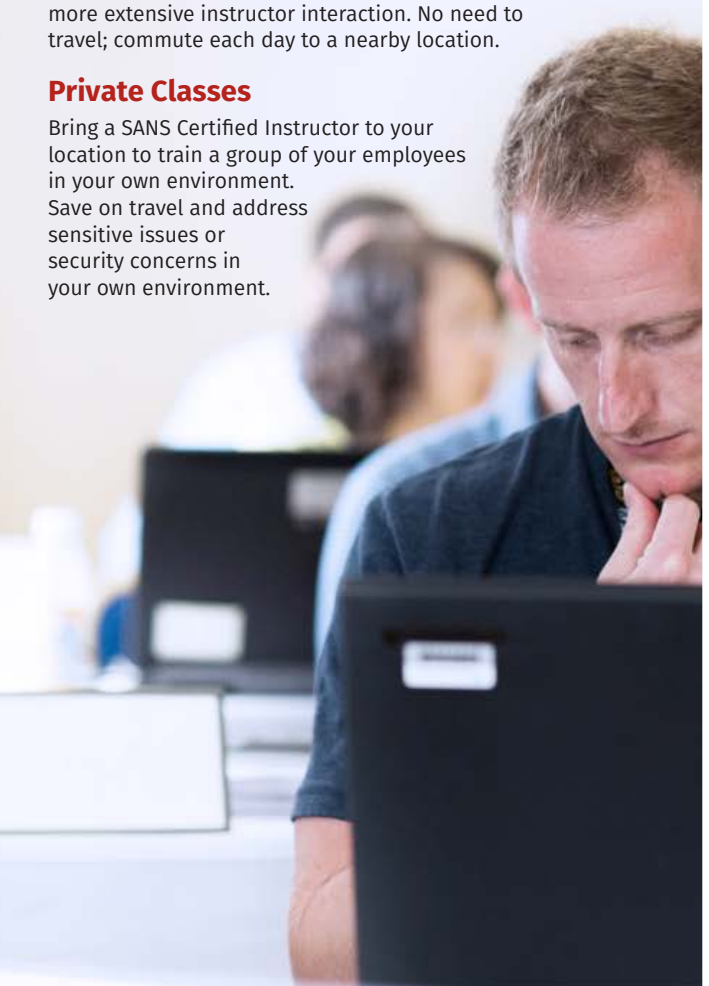
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses

Same SANS courses, courseware, and labs, taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes

Bring a SANS Certified Instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.



Online Training

SANS Online successfully delivers the same measured learning outcomes to students at a distance that we deliver live in classrooms. More than 30 courses are available for you to take whenever or wherever you want. Thousands of students take our courses online each year and frequently achieve certification.

Top reasons to take SANS courses online:

- Learn at your own pace, over four months
- Spend extra time on complex topics
- Repeat labs to ensure proficiency with skills
- Save on travel costs
- Study at home or in your office

Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

"The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life."

-Dan Trueman, Novae PLC

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, June 12 - Sat, June 17
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Jonathan Ham

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Learn to build a security roadmap that can scale today and into the future!

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. This course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

With the rise of advanced persistent threats, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- What is the risk?
- Is it the highest priority risk?
- What is the most cost-effective way to reduce the risk?

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you'll need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

www.giac.org/gsec

SANS Technology Institute
www.sans.edu

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"Between the knowledge of the instructor and the application of course material, everything was run to perfection!"
-Joe Lordi, Wawa, Inc.

Jonathan Ham *SANS Certified Instructor*

Jonathan is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 20 years, advising in both the public and private sectors, from small start-ups to the Fortune 500. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the CIRT for one of the largest U.S. civilian federal agencies. He has held the CISSP, GSEC, GCIA, and GCIH certifications, and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross. @jhamcorp

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, June 12 - Sat, June 17
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Mick Douglas

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), 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, attackers are targeting your systems with increasing viciousness and stealth. **As defenders, it is essential we understand these hacking tools and techniques.**

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 you love cybersecurity and learning how exploits work, you NEED this course!"
-Jaid, U.S. Navy

This course enables you to turn the tables on computer attackers by helping you understand their 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. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare for, detect, and respond to attacks. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a **hands-on** workshop that focuses on scanning, exploiting, and defending systems. This will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. **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.**

"This class prepares you for anything and everything that comes your way as a security professional that is asked to respond to various incidents."
-Matthew Nappi, Stony Brook University

www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

Mick Douglas *SANS Instructor*

Even when his job title has indicated otherwise, Mick Douglas has been doing information security work for over 10 years. He received a bachelor's degree in communications from Ohio State University and holds the CISSP, GCIH, GPEN, GCUX, GWEB, and GSNA certifications. He currently works at Binary Defense Systems as the DFIR Practice Lead. He is always excited for the opportunity to share with others so they do not have to learn the hard way! By studying with Mick, security professionals of all abilities will gain useful tools and skills that should make their jobs easier. When he's not "geeking out" you'll likely find Mick indulging in one of his numerous hobbies: photography, scuba diving, or hanging around in the great outdoors. @BetterSafetyNet

SEC560:

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, June 12 - Sat, June 17
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Jeff McJunkin

www.giac.org/gpen

www.sans.edu

www.sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"Learning how attackers profile and exploit allows me to understand how to tailor our product offerings to provide real value."
-Travis Smith, Tripwire

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with **over 30 detailed hands-on labs** throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently…and masterfully.

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser-known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. **You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.**

Who Should Attend

- Security personnel whose jobs involve assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

Jeff McJunkin *SANS Instructor*

Jeff McJunkin is a senior staff member at Counter Hack Challenges with more than nine years of experience in systems and network administration and network security. His greatest strength is his breadth of experience – from network and web application penetration testing to digital/mobile forensics, and from technical training to systems architecture. Jeff is a computer security/information assurance graduate of Southern Oregon University and holds many professional certifications. He has also competed in many security competitions, including taking first place at a regional NetWars competition and a U.S. Cyber Challenge capture-the-flag competition, as well as joining the Red Team for the Pacific Rim Collegiate Cyber Defense Competition. His personal blog can be found at http://jeffmcjunkin.com. @jeffmcjunkin

FOR408:
Windows Forensic Analysis

SANS

Six-Day Program
Mon, June 12 - Sat, June 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Carlos Cajigas

Master Windows Forensics – You can't protect what you don't know about.

Every organization must prepare for cyber crime occurring on its computer systems and within its networks. Demand has never been greater for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

"The Windows registry forensic section blew my mind! I didn't think it stored that much information." -Tung Nguyen, Denver Water

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. Understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

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

www.giac.org/gcfe

www.sans.edu

Bundle OnDemand
with this course
www.sans.org/ondemand

"The methods taught and the tools introduced will be very beneficial to me as an analyst performing examinations."
-Joseph Selph, IBM

Carlos Cajigas *SANS Certified Instructor*

As an incident responder, cybercrimes investigator, digital forensics trainer, and retired detective, Carlos has amassed a wealth of experience in high-technology crime investigations. As a detective with the West Palm Beach Police Department, he specialized in computer crime investigations. He has conducted examinations on hundreds of digital devices to go along with hundreds of hours of digital forensics training. His training includes courses by Guidance Software (EnCase), National White Collar Crime Center (NW3C), Access Data (FTK), United States Secret Service (USSS), IACIS, and SANS. Carlos holds bachelor's and master's degrees from Palm Beach Atlantic University (FL). In addition, he holds various certifications in the digital forensics field, including EnCase Certified Examiner (EnCE), Certified Forensic Computer Examiner (CFCE) from IACIS, and the GCFE and GCFA. He is currently an incident responder for a Fortune 500 company, where he is responsible for responding to computer and network security threats for clients in North and South America. @Carlos_Cajigas

ICS410:
ICS/SCADA Security Essentials

SANS

Five-Day Program
Mon, June 12 - Fri, June 16
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Eric Cornelius

www.giac.org/gicsp

www.sans.edu

Bundle OnDemand
with this course
www.sans.org/ondemand

Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

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. **ICS410: 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.

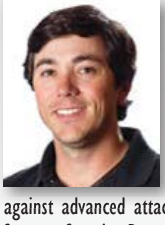
The course will provide you with:

- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

"This course was a great introduction into the ICS landscape and associated security concerns. The ICS material presented will provide immediate value relative to helping secure my company." -Mike Poulos, Coca-Cola Enterprises

Given the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. In addition, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity.



Eric Cornelius *SANS Certified Instructor*

Eric Cornelius is the Director of Critical Infrastructure and Industrial Control Systems (ICS) at Cylance, Inc., where he is responsible for thought leadership, architecture, and consulting. Eric brings a wealth of ICS knowledge and his leadership keeps organizations safe, secure, and resilient against advanced attackers. Previously, Eric served as the Deputy Director and Chief Technical Analyst for the Control Systems Security Program at the U.S. Department of Homeland Security. Eric earned a bachelor's degree from the New Mexico Institute of Mining and Technology, where he was the recipient of many scholarships and awards including the National Science Foundation's Scholarship for Service. Eric went on to work at the Army Research Laboratory's (ARL) Survivability/Lethality Analysis Directorate, where he worked to secure field-deployable combat technologies. It was at ARL that Eric became interested in non-traditional computing systems, an interest that ultimately led him to the Idaho National Laboratory where he participated in deep-dive vulnerability assessments of a wide range of ICS systems. Eric is the co-author of "Recommended Practice: Creating Cyber Forensics Plans for Control Systems" as part of the DHS National Cyber Security Division's 2008 Control Systems Security Program and is also a frequent speaker and instructor at ICS events across the globe.

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

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

Virtualizing Forensic Images Using Free Tools in Linux

Carlos Cajigas

Have you ever needed to boot a forensic image to preview the system in a live manner? Would you like to do it without changing a single bit? It is possible! In this session we will discuss the tools and steps required for converting the Donald Blake forensic image into a Virtual Machine (VM). This process is useful, because it gives you the ability to boot an image of an OS drive into a VM, all while preserving the integrity of the image. All changes made by the OS are saved and stored to a cache file. Come see how you accomplish this using free tools under Linux Ubuntu. The presentation will include a live demo.

Becoming a Better Technologist by Becoming Better at Business

Eric Cornelius

We in the technical world often refer to ourselves as "ninjas" or "wizards" because of the technical sorcery our teams are able to conjure. However, we are often frustrated when our recommendations fall on deaf ears at the board level, often by an audience that "just doesn't get it." This talk will offer an alternative thesis that suggests that perhaps it is the technical team that doesn't get it. Eric will focus on ways to effectively communicate technical concepts to business leaders and present our recommendations in the one context that all companies understand – money.

Building Your Own Kickass Home Lab

Jeff McJunkin

Building your own home lab is a great way to keep up with the ever-changing IT world. But, how does one actually go about building a home lab? That's the part that gets more complicated. Do you really need a whole rack full of off-lease servers and some enterprise-grade switches? No! New-ish high-end servers and workstations are surprisingly powerful, capable of mocking up a pretty complicated network, including attacker systems and even incorporating wireless communications. In this talk, Jeff will walk through both the hardware and software stacks he uses and recommends, including a number of ways to incorporate Microsoft software without paying exorbitant licensing fees. Jeff will also outline a basic lab design that can be used for a number of scenarios.

Enhance Your Training Experience

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days of this event for just $689 each.

SPECIAL PRICING

Extend Your Training Experience with an OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter-expert support to help you increase your retention of course material

"The course content and OnDemand delivery method have both exceeded my expectations."

-Robert Jones, Team Jones, Inc.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt

"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, Department of Commerce

MORE INFORMATION

www.sans.org/ondemand/bundles www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.

Securing **Approval** and **Budget** for Training

Packaging matters

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Clearly state the benefits

Be specific

- How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled "You Will Be Able To." Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Set the context

Establish longer-term expectations

- Information security is a specialized career path within IT, with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense, and not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of learning that passing a GIAC exam offers. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expense into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.

SANS VOUCHER PROGRAM

The SANS Voucher Program allows an organization to manage its training budget from a single SANS Account, potentially receive bonus funds based on its investment level, and centrally administer its training.

Training Investment & Bonus Funds

To open a Voucher Account, an organization pays an agreed-upon training investment. Based on the amount of the training investment, an organization could be eligible to receive bonus funds.

The investment and bonus funds:

- Can be applied to **any live or online SANS training course, SANS Summit, GIAC certification, or certification renewal***
- Can be increased at any time by making additional investments
- Need to be utilized within 12 months, however, the term can be extended by investing additional funds before the end of the 12-month term

*Current exceptions are the Partnership Program, Security Awareness Training, and SANS workshops hosted at events and conferences run by other companies.

Flexibility & Control

The online SANS Admin Tool allows the organization's Program Administrator to manage the account at anytime from anywhere.

With the SANS Admin Tool, the Administrator can:

- Approve student enrollment and manage fund usage
- View fund usage in real time
- View students' certification statuses and test results
- Obtain OnDemand course progress by student per course

By creating a Voucher Account, your organization can:

- Simplify the procurement process with a single invoice and payment
- Easily change course attendees if previous plans change
- Lock-in your hard fought training budget and utilize it over time
- Control how, where, and for whom funds are spent
- Allow employees to register for training while managing approvals centrally

Getting Started

Complete and submit the form online at **www.sans.org/vouchers** and a SANS representative in your region will contact you within 24 business hours.

Get started today and within as little as one week, we can create your Account and your employees can begin their training.

SANS SECURING THE HUMAN

Security Awareness Training by the Most Trusted Source

Computer-based Training for Your Employees

End User
CIP v5
ICS Engineers
Developers
Healthcare

- Let employees train on their own schedule
- Tailor modules to address specific audiences
- Courses translated into many languages
- Test learner comprehension through module quizzes
- Track training completion for compliance reporting purposes

Visit SANS Securing The Human at
securingthehuman.sans.org

Phishing | Knowledge Assessments | Culture and Behavior Change | Managed Services

SANS Technology Institute

The SANS Technology Institute transforms the world's best cybersecurity training and certifications into a comprehensive and rigorous graduate education experience.

Master's Degree Programs:

- M.S. in Information Security Engineering
- M.S. in Information Security Management

Specialized Graduate Certificates:

- Cybersecurity Engineering (Core)
- Cyber Defense Operations
- Penetration Testing and Ethical Hacking
- Incident Response

SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education.
3624 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

GI Bill.

Eligible for veterans education benefits!
Earn industry-recognized GIAC certifications throughout the program.
Learn more at **www.sans.edu** | **info@sans.edu**

GIAC CERTIFICATIONS

GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA).
More information about education benefits offered by VA is available at the official U.S. government website at www.benefits.va.gov/gibill.

Future Training Events

Pen Test Austin . . . . . Austin, TX . . . . . Mar 27 - Apr 1

SANS 2017 . . . . . Orlando, FL . . . . . Apr 7-14

Baltimore Spring . . . . . Baltimore, MD . . . . . Apr 24-29

Security West . . . . . San Diego, CA . . . May 9-18

Northern Virginia – Reston . . . . Reston, VA . . . . . May 21-26
Atlanta . . . . . Atlanta, GA . . . . . May 30 - June 4
Houston . . . . . Houston, TX . . . . . June 5-10
San Francisco Summer . . . . . San Francisco, CA . . . . . June 5-10
Rocky Mountain . . . . . Denver, CO . . . . . June 12-17
Charlotte . . . . . Charlotte, NC . . . . . June 12-17
Minneapolis . . . . . Minneapolis, MN . . . . . June 19-24
Columbia . . . . . Columbia, MD . . . . . June 26 - July 1
Los Angeles - Long Beach . . . . . Long Beach, CA . . . . . July 10-15

SANSFIRE . . . . . Washington, DC July 22-29

San Antonio . . . . . San Antonio, TX . . . . . Aug 6-11
Boston . . . . . Boston, MA . . . . . Aug 7-12
New York City . . . . . New York, NY . . . . . Aug 14-19
Salt Lake City . . . . . Salt Lake City, UT . . . . . Aug 14-19
Chicago . . . . . Chicago, IL . . . . . Aug 21-26
Virginia Beach . . . . . Virginia Beach, VA . . . Aug 21 - Sep 1
Tampa - Clearwater . . . . . Clearwater, FL . . . . . Sep 5-10
San Francisco Fall . . . . . San Francisco, CA . . . . . Sep 5-10

Future Summit Events

Threat Hunting and IR . . . . . New Orleans, LA . . . . . Apr 18-25
Automotive Cybersecurity . . . . Detroit, MI . . . . . May 1-8
Security Operations Center . . . Washington, DC . . . . . June 5-12
Digital Forensics . . . . . Austin, TX . . . . . June 22-29
ICS & Energy . . . . . Houston, TX . . . . . July 10-14
Security Awareness . . . . . Nashville, TN . . . . . July 31 - Aug 9
Data Breach . . . . . Chicago, IL . . . . . Sep 25 - Oct 2

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit **www.sans.org/community** for up-to-date Community course information.

SANS CHARLOTTE 2017

Hotel Information

Training Campus

Hilton Charlotte University Place

8629 JM Keynes Drive
Charlotte, NC, 28262
704-547-7444
www.sans.org/event/charlotte-2017/location

Hilton Charlotte University Place offers a tranquil lakeside escape near UNC Charlotte and the area's best shopping destinations. Whether you're here for business or leisure, you'll appreciate this lakeside location just 15 miles from the Charlotte Douglas International Airport. Dine lakeside at the hotel's on-site restaurant, Edgewater Bar and Grille and enjoy stunning lake views from many of the guest rooms and meeting rooms.

Special Hotel Rates Available

A special discounted rate of $145.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through May 18, 2017. To book a room, please call 704-547-7444 and mention you are with SANS.

Top 5 reasons to stay at the Hilton Charlotte University Place

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 Hilton Charlotte University Place you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Hilton Charlotte University Place that you won't want to miss!
5. Everything is in one convenient location!

SANS CHARLOTTE 2017

Registration Information

We recommend you register early to ensure you get your first choice of courses.

Register online at www.sans.org/charlotte

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

Use code **EarlyBird17** when registering early

Pay Early and Save*

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**4-19-17**	**$400.00**	**5-10-17**	**$200.00**

*Some restrictions apply. Early-bird discounts do not apply to Hosted courses.

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by May 24, 2017 – processing fees may apply.

Open a **SANS Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert Webcasts – SANS experts bring current and timely information on relevant topics in IT Security.

Analyst Webcasts – A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts – The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

Tool Talks – Tool Talks are designed to give you a solid understanding of a problem, and to show how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

NewsBites – Twice-weekly high-level executive summary of the most important news relevant to cybersecurity professionals

OUCH! – The world's leading monthly free security-awareness newsletter designed for the common computer user

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/account