

SANS

Seattle 2016

October 3-8

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

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

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Six courses on
CYBER DEFENSE
PEN TESTING
DIGITAL FORENSICS
SECURITY MANAGEMENT
ICS SECURITY

“SANS courses give
you real-world
skills that have an
immediate value
on the security
environment.”

-ERIC KAITHULA, SYMETRA



GIAC-Approved
Training

**SAVE
\$400**

by registering
and paying early!
See page 13 for
more details.

www.sans.org/seattle

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 Seattle 2016 lineup of instructors includes:



Ted Demopoulos
Certified Instructor
@TedDemop



Matt Edmondson
SANS Instructor
@matt0177



Carlos Cajigas
SANS Instructor
@Carlos_Cajigas



Bryce Galbraith
Principal Instructor
@brycegalbraith



My-Ngoc Nguyen
Certified Instructor
@MenopN



Keith Palmgren
Senior Instructor
@kpalmgren



Billy Rios
SANS Instructor
@XSSniper

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 8.

KEYNOTE: *Everything You Ever Learned About Passwords Is Wrong* – Keith Palmgren

Python for OSINT Domination – Matt Edmondson

How to Bring Some Advanced Persistent Trickery to Your Fight Against Advanced Persistent Threats – Bryce Galbraith

Security Leadership for Everyone: Personal Authority and Beyond – Ted Demopoulos

The training campus for SANS Seattle 2016 is at the Renaissance Seattle, a stylish downtown hotel conveniently located just minutes from CenturyLink and Safeco Fields, Pike Place Market, and upscale shopping.

SEE PAGE 13



Be sure to register and pay by August 10th for a \$400 tuition discount!

Courses-at-a-Glance

	MON 10-3	TUE 10-4	WED 10-5	THU 10-6	FRI 10-7	SAT 10-8
SEC301 Intro to Information Security	Page 2					
SEC401 Security Essentials Bootcamp Style	Page 3					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 4					
FOR408 Windows Forensic Analysis	Page 5					
MGT514 IT Security Strategic Planning, Policy, and Leadership	Page 6					
ICS410 ICS/SCADA Security Essentials	Page 7					

Register today for SANS Seattle 2016!

www.sans.org/seattle



@SANSInstitute
Join the conversation:
#SANSSeattle

The Value of SANS Training & YOU



EXPLORE

- Read this brochure and note the courses that will enhance your role in your organization
- Use the Career Roadmap (www.sans.org/media/security-training/roadmap.pdf) to plan your growth in your chosen career path

RELATE

- Consider how security needs in your workplace will be met with the knowledge you'll gain in a SANS course
- Know the education you receive will make you an expert resource for your team

VALIDATE

- Pursue a GIAC Certification after your training to validate your new expertise
- Add a NetWars challenge to your SANS experience to prove your hands-on skills

SAVE

- Register early to pay less using early-bird specials
- Consider the SANS Voucher Program or bundled course packages to make the most of your training budget

ADD VALUE

- Network with fellow security experts in your industry
- Prepare thoughts and questions before arriving to share with the group
- Attend SANS@Night talks and activities to gain even more knowledge and experience from instructors and peers alike

ALTERNATIVES

- If you cannot attend a live training event in person, attend the courses virtually via SANS Simulcast
- Use SANS OnDemand or vLive to complete the same training online from anywhere in the world, at any time

ACT

- Bring the value of SANS training to your career and organization by registering for a course today, or contact us at 301-654-SANS with further questions

Return on Investment

SANS live training is recognized as the best resource in the world for information security education. With SANS, you gain significant returns on your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

REMEMBER

*the SANS promise:
You will be able to apply
our information security
training the day you get
back to the office!*

SEC301:

Intro to Information Security

Five-Day Program

Mon, Oct 3 - Fri, Oct 7

9:00am - 5:00pm

30 CPEs

Laptop Required

Instructor: My-Ngoc Nguyen


www.giac.org/gisf

**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand

“My-Ngoc was an excellent instructor and the basis for my new knowledge of computer cyber-crimes for law enforcement. This course will help with our investigation and detection of cyber-fraud in the field.”

-JUSTINE KILLEEN, NYPD


My-Ngoc Nguyen SANS Certified Instructor

My-Ngoc Nguyen (pronounced Mee-Nop Wynn) is the CEO/Principal Consultant for Secured IT Solutions. She has 15 years of experience in information systems and technology, with the past 12 years focused on cybersecurity and information assurance for both the government and commercial sectors. My-Ngoc is highly experienced in IT security and risk methodologies, and in legal and compliance programs. She led a cybersecurity program under a federal agency for a highly-regulated, first-of-a-kind project of national importance. With that experience, she has been assisting client organizations in both the public and private sectors to implement secure and compliant business processes and IT solutions using defense-in-depth and risk-based approaches. Along with a master's degree in management information systems, she carries top security certifications, including GPEN, GCIH, GSEC, and CISSP and is a former QSA. She is an active member of the FBI's InfraGard, the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC). My-Ngoc co-founded the non-profit public service organization CyberSafeNV to raise security awareness among Nevada residents and is presently the organization's chairperson. @MenopN

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- Are you new to information security and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Are you a non-IT security manager who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?

If you answer yes to any of these questions, the **SEC301: Introduction to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have no prior knowledge of security and limited knowledge of technology. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

“The instructor was exceptionally prepared for the course!

It was absolutely great work on her side!” -ALINA STOLINA, EY

Authored by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp**. It also delivers on the SANS promise: **You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.**

SEC401:

Security Essentials Bootcamp Style

Six-Day Program

Mon, Oct 3 - Sat, Oct 8

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

46 CPEs

Laptop Required

Instructor: Keith Palmgren


www.giac.org/gsec

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140
BUNDLE
ONDEMAND

WITH THIS COURSE

www.sans.org/ondemand

“The instructor did a really awesome job with crypto. It was the best explanation I have heard without overloading on tech jargon.”

-MIKE LAWRENCE, PROTIVITI

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. 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.



Keith Palmgren

SANS Senior Instructor

Keith Palmgren is an IT security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys and codes management. He also worked in what was at the time the newly-formed computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice, responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

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
- ▶ 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

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program

Mon, Oct 3 - Sat, Oct 8

9:00am - 7:15pm (Day 1)

9:00am - 5:00pm (Days 2-6)

37 CPEs

Laptop Required

Instructors: Bryce Galbraith

Matt Edmondson


www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

www.sans.org/ondemand

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

“SEC504 really puts the state of things in perspective – being proactive to combat the threats of the Internet.” -JONATHAN MANAFI, MCLHENNY COMPANY

This course helps you 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.**



Bryce Galbraith SANS Principal Instructor

As a contributing author of the international bestseller *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. He has held security positions at global ISPs and Fortune 500 companies, was a member of Foundstone's renowned penetration testing team, and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences worldwide. [@brycegalbraith](https://twitter.com/brycegalbraith)



Matt Edmondson SANS Instructor

Matt performs technical duties for the U.S. government and is a Principal at Argelius Labs, where he performs security assessments and consulting work. A recognized expert in his field with a knack for communicating complicated technical issues to students, both technical and non-technical, Matt routinely provides cybersecurity instruction to individuals from the Department of Defense, Department of Justice, Department of Homeland Security, Department of Interior, and other agencies. [@matt0177](https://twitter.com/matt0177)

FOR 408:

Windows Forensic Analysis

Six-Day Program

Mon, Oct 3 - Sat, Oct 8

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Carlos Cajigas

www.giac.org/gfcewww.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 Instructor

As an incident responder, retired detective, cybercrimes investigator, and digital forensics trainer, Carlos has amassed a wealth of experience in high-technology crime investigations. He was a detective with the West Palm Beach Police Department, where 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 GIAC Certifications 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

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.

“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

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

MGT 514:

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
 Mon, Oct 3 - Fri, Oct 7
 9:00am - 5:00pm
 30 CPEs
 Laptop NOT Needed
 Instructor: Ted Demopoulos



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

“This was excellent training with encyclopedic coverage of the topic, and the instructor was fantastic with lots of wisdom and real-life examples.”
 -ALEXANDER KOTKOV,
 ERNST AND YOUNG

“The balance is great and the full policy in the appendix helped to round out the analysis. The policy discussions and slides were quite helpful.”
 -JASON POPP, NORDSTROM INC.



Ted Demopoulos SANS Certified Instructor

Ted Demopoulos' first significant exposure to computers was in 1977 when he had unlimited access to his high school's PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been ongoing ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a “textbook failure” of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press. He also has written two books on social media, has an ongoing software concern in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. In his spare time, he is a food and wine geek, enjoys flyfishing, and plays with his children. @TedDemop

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

Who Should Attend

- ▶ CISOs
- ▶ Information security officers
- ▶ Security directors
- ▶ Security managers
- ▶ Aspiring security leaders
- ▶ Other security personnel who have team-lead or management responsibilities

This course teaches security professionals how to do three things:

▶ Develop Strategic Plans

Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.

▶ Create Effective Information Security Policy

Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, “No way, I am not going to do that?” Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.

▶ Develop Management and Leadership Skills

Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

ICS410: ICS/SCADA Security Essentials

Five-Day Program
Mon, Oct 3 - Fri, Oct 7
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Billy Rios



www.giac.org/gicsp



www.sans.edu

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

“The course content is excellent! I’ve learned a lot and the course has rejuvenated my interest in ICS security.”
-MARCEL P. ABLOG,
SAN ROQUE POWER

“The real-world relationship was key to applying the information. The instructor relates his experiences with the attacks.”
-TAYLOR A., MARFOR CYBER



Billy Rios SANS Instructor

An accomplished author and speaker, Billy is recognized as one of the world’s most respected experts on emerging threats related to industrial control systems (ICS), critical infrastructure, and, medical devices. He has discovered thousands of security vulnerabilities in hardware and software supporting ICS and critical infrastructure. He has been publicly credited by the Department of Homeland Security (DHS) over 50 times for his support to the DHS ICS Cyber Emergency Response Team (ICS-CERT). Billy was a Lead at Google, where he led the front-line response to externally reported security issues and incidents. Prior to Google, Billy was the Security Program Manager at Internet Explorer (Microsoft). During his time at Microsoft, Billy led the company’s response to several high-profile incidents, including the response for Operation Aurora. Before Microsoft, Billy worked as a penetration tester, an intrusion detection analyst, and served as an active duty Marine Corps Officer. Billy currently holds an MBA and a master’s of science degree in information systems. He was a contributing author for several publications including *Hacking, the Next Generation* (O’Reilly), *Inside Cyber Warfare* (O’Reilly), and *The Virtual Battle Field* (IOS Press). @XSSniper

SANS has joined forces with industry leaders **Who Should Attend**

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
- A license to Windows 10 and a hardware PLC for students to use in class and take home with them

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.

When students complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

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@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.

KEYNOTE:

Everything You Ever Learned About Passwords Is Wrong

Keith Palmgren

Perhaps the worst advice you can give a user is “choose a complex password.” The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves and even for their children.

Python for OSINT Domination

Matt Edmondson

In just about every engagement, the first step is reconnaissance and information gathering. There can be an overwhelming amount of information out there and anything you can do to automate the process of acquiring and analyzing it will make your life a lot easier. This presentation will start with simple data mining techniques where APIs and basic scraping can be utilized, before addressing possible challenges to an automated approach, such as sites that require user interaction to log in, click buttons, scroll down, etc. Working proof of concept code will be provided for all of the topics discussed.

How to Bring Some Advanced Persistent Trickery to Your Fight Against Advanced Persistent Threats

Bryce Galbraith

You know you have intruders on your computer...but this is your computer and no one knows it better than you. Don't sit back and wait...It's game on! This presentation will explore ways that you can frustrate, annoy, and potentially reveal advanced persistent threats (APTs) with active defense, offensive countermeasures, and cyber deception (legally and ethically).

Security Leadership For Everyone: Personal Authority and Beyond

Ted Demopoulos

Security leadership is not a role for only those in charge. A leader is anyone who has followers: they may have followers because they are in a position of power; because they take initiative, or perhaps simply because they set a good example and people follow their lead. Leaders have followers because they have some sort of “authority.” Or they may have “positional authority” because they are in charge, or because of their position or title. They may have “personal authority,” authority that is earned through actions. Many leaders have both: positional authority because they are in charge and personal authority because they have earned respect through their actions. In this presentation, part of the Infosec Rock Star series of talks, we look at leadership and authority, discussing both types of authority and concentrating on what it takes to establish personal authority in security. Security leadership is not reserved for those “in charge” – personal authority can be earned by all of us.



Security Awareness Training by the Most Trusted Source

Computer-based Training for Your Employees

- End User** • Let employees train on their own schedule
- CIP v5/6** • Tailor modules to address specific audiences
- ICS Engineers** • Courses translated into many languages
- Developers** • Test learner comprehension through module quizzes
- Healthcare** • Track training completion for compliance reporting purposes

Visit SANS Securing The Human at
securingthehuman.sans.org



Change Human Behavior | Manage Risk | Maintain Compliance | Protect Your Brand

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.



Eligible for VA education benefits!

Earn industry-recognized GIAC certifications throughout the program.

Learn more at www.sans.edu | info@sans.edu



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.

Enhance Your Training Experience

WITH

Even More Training Value

Add an
OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days
of this event for just \$659 each.

SPECIAL
PRICING



Extend Your Training Experience with **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 Certification**

- Distinguish yourself as an information security leader
- 30+ GIAC certifications to choose from
- 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

Employers need good talent.
Veterans need good jobs.
SANS VetSuccess Immersion Academy
delivers both.

Introducing the SANS VetSuccess Immersion Academy, an intensive, accelerated program that provides the real-world training and certifications needed to fill critical jobs in cybersecurity.

For employers, the academy is a faster, more reliable, and less expensive way to find, train, certify, and employ highly qualified cybersecurity talent.

For transitioning veterans, the academy provides free accelerated training and certifications to quickly and effectively launch careers in cybersecurity.

Find out how your organization can benefit from hiring graduates or sponsoring an academy to meet your specific talent needs.

Read the Pilot Program Results Report
Visit sans.org/vetsuccess

SANS | CyberTalent
IMMERSION ACADEMY



*Read the Pilot Program
Results Report*
Visit sans.org/vetsuccess

*Women's Academy Pilot
1st cohort graduation
Summer 2016*



VetSuccess

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING



Multi-Course Training Events www.sans.org/security-training/by-location/all
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers



Community SANS www.sans.org/community
Live Training in Your Local Region with Smaller Class Sizes



Private Training www.sans.org/private-training
Live Onsite Training at Your Office Location. Both In-person and Online Options Available



Mentor www.sans.org/mentor
Live Multi-Week Training with a Mentor



Summit www.sans.org/summit
Live IT Security Summits and Training

ONLINE TRAINING



OnDemand www.sans.org/ondemand
E-learning Available Anytime, Anywhere, at Your Own Pace



vLive www.sans.org/vlive
Online Evening Courses with SANS' Top Instructors



Simulcast www.sans.org/simulcast
Attend a SANS Training Event without Leaving Home



OnDemand Bundles www.sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

FUTURE SANS TRAINING EVENTS

ICS Security Training – Houston 2016

Houston, TX | Jul 25-30

San Jose 2016

San Jose, CA | Jul 25-30

Boston 2016

Boston, MA | Aug 1-6

Security Awareness SUMMIT & TRAINING 2016

San Francisco, CA | Aug 1-10

Portland 2016

Portland, OR | Aug 8-13

Dallas 2016

Dallas, TX | Aug 8-13

Data Breach SUMMIT

Chicago, IL | Aug 18

Chicago 2016

Chicago, IL | Aug 22-27

Virginia Beach 2016

Virginia Beach, VA | Aug 22 - Sep 2

NORTHERN VIRGINIA

Crystal City 2016

Crystal City, VA | Sep 6-11

Network Security 2016

Las Vegas, NV | Sep 10-19

Security Leadership SUMMIT & TRAINING 2016

Dallas, TX | Sep 27 - Oct 4

Baltimore 2016

Baltimore, MD | Oct 10-15

Cyber Defense San Diego 2016

San Diego, CA | Oct 23-28

Information on all events can be found at
www.sans.org/security-training/by-location/all

Hotel Information

Training Campus

Renaissance Seattle Hotel

515 Madison Street

Seattle, WA 98104 | 800-546-9184

www.sans.org/event/seattle-2016/location



Experience the Renaissance Seattle, a stylish downtown hotel conveniently located just minutes from CenturyLink and Safeco Fields, Pike Place Market and upscale shopping. Staying at the Renaissance Seattle Hotel eliminates any travel stress thanks to easy access to major freeways and Sea-Tac International Airport. Unwind in spacious and newly renovated guest rooms. The hotel features colorful paintings by local artists displayed in the lobby, a fully equipped fitness center, and high-speed Internet. Discover how our hotel seamlessly combines luxury, comfort and technology into an unforgettable urban retreat.

Special Hotel Rates Available

A special discounted rate of \$209.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through September 12, 2016.

Top 5 reasons to stay at the Renaissance Seattle Hotel

- 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 Renaissance Seattle Hotel 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 Renaissance Seattle Hotel that you won't want to miss!
- 5 Everything is in one convenient location!

Registration Information

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



Register online at www.sans.org/seattle

Select your course or courses 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.

Pay Early and Save

Use code **EarlyBird16** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	8-10-16	\$400.00	8-31-16	\$200.00

Some restrictions apply.

SANS Voucher Program

Expand your training budget!

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.




www.sans.org/vouchers

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 September 14, 2016 — 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/security-resources