THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS

Capital City 2013

Washington, DC | September 3-8, 2013

> *"This was an awesome and informative experience. My organization will benefit as a result. Thanks!"*
>
> -Far'd Thomas, Lockheed Martin

Hands-on immersion training programs, including:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Web App Penetration Testing and Ethical Hacking

SANS Security Leadership Essentials For Managers

Intrusion Detection In-Depth

Intro to Information Security

GIAC Approved Training

Register at www.sans.org/event/sans-capital-city-2013

Save $500 by registering early!

See page 13 for more details.

Stephen Northcutt

Dear Colleagues,

We would like to invite you to Washington, DC for another outstanding offering of IT security and security managment courses at the **Grand Hyatt Washington on September 3-8**.

Make your plans now to attend **SANS Capital City 2013** for six of our top courses brought to you by instructors who are also industry practitioners. Explore this brochure for course descriptions and instructor bios for Dr. Eric Cole, Fred Kerby, Mike Poor, Kevin Fiscus, Timothy Tomes, and G. Mark Hardy, our teaching team, who will ensure that you can use what you learn in the classroom as soon as you return to the office.

All six courses are associated with the prestigious *GIAC Certification*. To turbo-charge your career, check which courses can help you earn your master's degree at the *SANS Technology Institute* (STI). Find out about more about GIAC and STI in this brochure.

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

- **Keynote: Who's Watching the Watchers?** *presented by Mike Poor*
- **GIAC Program Overview**
- **SANS Technology Institute Open House**
- **Look Ma, No Exploits! - The Recon-ng Framework** *presented by Tim Tomes*
- **How the West was Pwned** *presented by G. Mark Hardy*
- **A Beginner's Guide to Cryptography Through Python** *presented by Kevin Fiscus*
- **Vendor Showcase events**

SANS training is well-known for being relevant and pragmatic. Our award-winning faculty has proven they understand the challenges you face on a daily basis. Their real-world experience increases the practical value of the course material.

Our campus for this event, the Grand Hyatt Washington, is located in the Penn Quarter, which will allow you to explore the U.S. Capitol, historic monuments, or the Smithsonian Museums. A discounted room rate of $189 Single/Double is available to SANS students until August 12, but space is limited so book early!

Washington, DC is a fabulous destination for training with all that there is to do. Places to visit include:

- **National Mall**
- **President Lincoln's Cottage**
- **Library of Congress**
- **Smithsonian National Air and Space Museum**
- **National Portrait Gallery**
- **National Zoo**
- **Lincoln Memorial**
- **Washington Monument**
- **Arlington National Cemetery**
- **Vietnam Veterans Memorial Wall**
- **National Postal Museum**
- **See the original Declaration of Independence, the U.S. Constitution, and the Bill of Rights at the National Archives**
- **The Ford Theatre, Newseum, National Gallery of Art, Shakespeare Theatre Company, and Verizon Center are all right in the Penn Quarter**
- **And so much more –** *see http://washington.org*

Register and pay by July 24 and receive a $500 tuition fee discount! Start making your training and travel plans now; let your colleagues and friends know about SANS Capital City 2013!

Stephen Northcutt

Stephen Northcutt
SANS Faculty Fellow

Here is what past attendees had to say about their SANS training:

"SANS continues to amaze with the depth and breadth of information they throw at you in a very short time. It's amazing how much sticks!"

-David Marek,
College of Southern Maryland

"Got SANS? I love this stuff. I am a believer. . . Now, if I can just convince my bosses to do it!"

-Bill Coffey, Shaw AFB

"Every SANS course I have taken has been world-class. This one is no different."

-Eric Robinson,
Premera Blue Cross

Courses-at-a-Glance

<table>
<tr><th></th><th></th><th>TUE
9/3</th><th>WED
9/4</th><th>THU
9/5</th><th>FRI
9/6</th><th>SAT
9/7</th><th>SUN
9/8</th></tr>
<tr><td>SEC301</td><td>Intro to Information Security</td><td colspan="5">PAGE 1</td><td></td></tr>
<tr><td>SEC401</td><td>Security Essentials Bootcamp Style</td><td colspan="6">PAGE 2</td></tr>
<tr><td>SEC503</td><td>Intrusion Detection In-Depth</td><td colspan="6">PAGE 3</td></tr>
<tr><td>SEC504</td><td>Hacker Techniques, Exploits, and Incident Handling</td><td colspan="6">PAGE 4</td></tr>
<tr><td>SEC542</td><td>Web App Penetration Testing and Ethical Hacking</td><td colspan="6">PAGE 5</td></tr>
<tr><td>MGT512</td><td>SANS Security Leadership Essentials For Managers</td><td colspan="5">PAGE 6</td><td></td></tr>
</table>

SECURITY 301

Intro to Information Security

Five-Day Program • Tue, Sept 3 – Sat, Sept 7
9:00am – 5:00pm • Laptop NOT Required
30 CPE/CMU Credits • Instructor: Fred Kerby

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and the basics of risk management. Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, Security 301 is the course for you!

We begin by covering basic terminology and concepts, and then move to the basics of computers and networking as we discuss Internet Protocol, routing, Domain Name Service, and network devices. We cover the basics of cryptography, security management, and wireless networking, then we look at policy as a tool to effect change in your organization. On the final day of the course, we put it all together with an implementation of defense in-depth.

This course will help you develop the skills to bridge the gap that often exists between managers and system administrators, and learn to communicate effectively with personnel in all departments and at all levels within your organization.

Who Should Attend:

- Persons new to information technology who need to understand the basics of information assurance, computer networking, cryptography, and risk evaluation
- Managers and Information Security Officers who need a basic understanding of risk management and the tradeoffs between confidentiality, integrity, and availability
- Managers, administrators, and auditors who need to draft, update, implement, or enforce policy

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/sans-capital-city-2013.

> *"Great crash-course and immersion for security and technology! From the logistics to the IS and OS, the necessary pieces of the cyber security puzzle have come together."*
>
> -Ansley LaBarre, EWA/IIT

Fred Kerby *SANS Senior Instructor*

Fred is an engineer, manager, and security practitioner whose experience spans several generations of networking. He was the Information Assurance Manager at the Naval Surface Warfare Center, Dahlgren Division for more than sixteen years. His team is one of the recipients of the SANS Security Technology Leadership Award as well as the Government Technology Leadership Award. Fred received the Navy Meritorious Civilian Service Award in recognition of his technical and management leadership in computer and network security. A frequent speaker at SANS, Fred's presentations reflect his opinions and are not the opinions of the Department of the Navy.

GIAC INFORMATION SECURITY FUNDAMENTALS GISF

www.giac.org

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program • Tue, Sept 3 - Sun, Sept 8
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Dr. Eric Cole

It seems wherever you turn organizations are being broken into and the fundamental question that everyone wants answered is: Why? Why is it that some organizations get broken into and others not? SEC401 Security Essentials is focused on teaching you the right things that need to be done to keep an organization secure. Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation but the right things will stop your organization from being headline news in the *Wall Street Journal*. SEC401's focus is to teach individuals the essential skills and techniques needed to protect and secure an organization's critical information assets and business systems. We also understand that security is a journey and not a destination. Therefore we will teach you how to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will have the techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure.

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, penetration testers, auditors who need a solid foundation of security principles so they can be effective as possible at their jobs**
- **Anyone new to information security with some background in information systems and networking**

With the APT (advanced persistent threat), organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While 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 works in cyber security. 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 cyber security, three questions must be answered:

1. **What is the risk?**
2. **Is it the highest priority risk?**
3. **Is it the most cost-effective way of reducing the risk?**

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401 you will learn the language and underlying theory of computer security. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security so that you will be prepared 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 gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defense. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including ***Advanced Persistent Threat***, ***Hackers Beware***, ***Hiding in Plain Site***, ***Network Security Bible*** 2nd Edition, and ***Insider Threat***. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty fellow and course author who works with students, teaches, and develops and maintains courseware.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/sans-capital-city-2013.

GIAC SECURITY ESSENTIALS CERTIFICATION GSEC

www.giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE

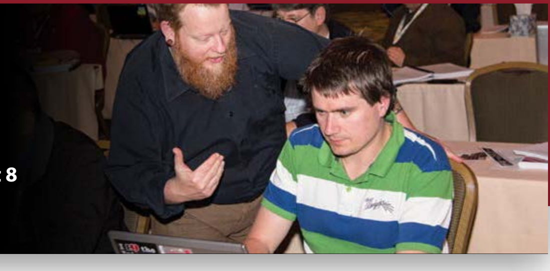
www.sans.edu

sapere aude

www.sans.org/cyber-guardian

SECURITY 503

Intrusion Detection In-Depth



Six-Day Program • Tue, Sept 3 - Sun, Sept 8
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Mike Poor

If you have an inkling of awareness of security (even my elderly aunt knows about the perils of the Interweb!), you often hear the disconcerting news about another high-profile company getting compromised. The security landscape is continually changing from what was once only perimeter protection to a current exposure of always-connected and often-vulnerable. Along with this is a great demand for security savvy employees who can help to detect and prevent intrusions. That is our goal in the Intrusion Detection In-Depth course – to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

Who Should Attend:

- **Intrusion detection analysts (all levels)**
- **Network engineers**
- **System, security, and network administrators**
- **Hands-on security managers**

This course spans a wide variety of topics from foundational material such as TCP/IP to detecting an intrusion, building in breadth and depth along the way. It's kind of like the "soup to nuts" or bits to bytes to packets to flow of traffic analysis.

"Mike Poor's ability to explain GCIA concepts is unmatched and will allow any junior analyst to hit the ground running."

-Erich Melcher, Sabre Systems, Inc.

"This course is valuable for anyone interested in IDS. Mike's knowledge and willingness to help you understand the material are unlike any other training I've been to. Great course and instructor."

-Dannie Arnold, U.S. Army

Hands-on exercises supplement the coursebook material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VMware distribution created by industry practitioner and SANS instructor Mike Poor. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. All exercises have two different approaches – a more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material to have a more challenging experience. Additionally, there is an "extra credit" stumper question for each exercise intended to challenge the most advanced student.

By week's end, your head should be overflowing with newly gained knowledge and skills; and your luggage should be swollen with course book material that didn't quite get absorbed into your brain during this intense week of learning. This course will enable you to "hit the ground running" once returning to a live environment.

"This course provides a good basis of knowledge and presents important tools which will be at the core of any intrusion analysis."

-Thomas Kelly, DIA

Mike Poor *SANS Senior Instructor*

Mike is a founder and senior security analyst for the Washington D.C. firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading their intrusion analysis team. As a consultant Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is in intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best selling ***Snort*** series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center.

"Course was designed around real-world intrusions and is highly needed for network security administrators and/or analysts."

-Hector Araiza, USAF

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/sans-capital-city-2013.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Tue, Sept 3 - Sun, Sept 8
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
Laptop Required • 37 CPE/CMU Credits
Instructor: Kevin Fiscus

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

> *"When I get back to the office, I will use the knowledge I gained here to better defend my organization's network."*
> -Joshua Anthony, West Virginia Army National Guard

Who Should Attend:

- Incident handlers
- Penetration testers
- Ethical hackers
- 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

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

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/sans-capital-city-2013.

> *"The course covers almost every corner of attack and defense areas. It's a very helpful handbook for a network security analysis job. It upgrades my knowledge in IT security and keeps pace with the trend."*
> -Anthony Liu, Scotia Bank

Kevin Fiscus *SANS Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. Kevin currently holds the CISA, GPEN, GREM, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has taught many of SANS most popular classes including SEC401, SEC504, SEC575, FOR508, and MGT414. In addition to his security work, he is a proud husband and father of two children.

> *"Fantastic class! Fantastic Instructor! I have taken six SANS classes, I have not had a bad experience yet, they are just so professionally done!"*
> -Rafael Cabrera, Air Force

GIAC CERTIFIED INCIDENT HANDLER GCIH
www.giac.org

SANS TECHNOLOGY INSTITUTE
www.sans.edu

www.sans.org/cyber-guardian

SECURITY 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program • Tue, Sept 3 - Sun, Sept 8
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Timothy Tomes

Assess Your Web Apps in Depth

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

> *"Fun while you learn! Just don't tell your manager. Every class gives you invaluable information from real world testing you cannot find in a book."*
>
> -David Fava, The Boeing Company

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

By knowing your enemy, you can defeat your enemy. General security practitioners, as well as website designers, architects, and developers, will benefit from learning the practical art of web application penetration testing in this class.

Who Should Attend:

- **General security practitioners**
- **Penetration testers**
- **Ethical hackers**
- **Web application vulnerability**
- **Website designers and architects**
- **Developers**

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/sans-capital-city-2013.

> ***"SEC542 is a step-by-step introduction to testing and penetrating web applications, a must for anyone who builds, maintains, or audits web systems."***
>
> -Brad Milhorn, ii2P LLC

Timothy Tomes *SANS Instructor*

Tim Tomes is a Senior Security Consultant and Developer for Black Hills Information Security with experience in information technology and application development. A veteran, Tim spent several years as an Officer in the United States Army conducting various information security related activities. Tim manages multiple open source projects such as the Recon-ng Framework, the HoneyBadger Geolocation Framework, and PushPin, is a SANS Instructor for SEC542 Web Application Penetration Testing, writes technical articles for PaulDotCom, and frequently presents at information security conferences.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Tue, Sept 3 – Sat, Sept 7
9:00am - 6:00pm (Course Days 1-4) • 9:00am - 4:00pm (Course Day 5)
33 CPE/CMU Credits • Laptop NOT Required • Instructor: G. Mark Hardy

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

Who Should Attend:

- All newly appointed information security officers
- Technically skilled administrators who have recently been given leadership responsibilities
- Seasoned managers who want to understand what your technical people are telling you

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

> *"Tremendously valuable experience!! Learned a lot and also validated a lot of our current pratices. Thank you!!"*
> -Chad Gray, Booz Allen Hamilton

> *"Every IT security professional should attend no matter what their position. This information is important to everyone."*
> -John Flood, NASA

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 Sailors. He also served as wartime Director, Joint Operations Center for US Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, a Masters in Business Administration, a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM, and CISA certifications.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/sans-capital-city-2013.

GIAC SECURITY LEADERSHIP CERTIFICATION GSLC

www.giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE

www.sans.edu

Bonus Sessions

SANS@Night Evening Talks

Enrich your SANS training experience! Evening talks given 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: **Who's Watching the Watchers?** *Mike Poor*

We have instrumented our networks to the Nth degree. We have firewalls, IDS, IPS, Next Gen Firewalls, Log correlation and aggregation... but do we know if we have it right? Will we detect the NextGen™ attackers?

In this talk we will explore ways that we improve the signal/noise ratio in our favor, and help identify the needle in the needlestack.

Look Ma, No Exploits! - The Recon-ng Framework *Tim Tomes*

I've been on the conference circuit for the last year preaching the importance of thorough reconnaissance as a part of the penetration testing methodology. I've talked about the principles of reconnaissance, how to accomplish it quickly and effectively, and even released a few tools to help along the way. In my latest tool, the Recon-ng framework, the power of reconnaissance has been taken to a new level. In this talk, I am going to discuss and demonstrate the power of the Recon-ng framework by walking attendees through a live reconnaissance scenario which starts with the tester having nothing but the framework, and ends with the tester gaining credentials to the target environment. All without sending a single packet to the target network. Come a skeptic. Leave a believer. Reconnaissance is king.

How the West was Pwned *G. Mark Hardy*

Can you hear it? The giant sucking sound to the East? With it are going more than just manufacturing jobs -- it's our manufacturing know-how, intellectual property, military secrets, and just about anything you can think of. If we're so technologically advanced, how are the People's Republic of China (PRC) and others able to continue to pull this off? Why do we keep getting pwned at our own game?

The Mandiant APT1 report released in February detailed research into People's Liberation Army (PLA) Unit 61398 and their significant penetration into western networks. It was followed quickly by a series of political and diplomatic statements denouncing China's actions, which China flatly denied. Where's the truth? We'll try to find it.

There has been much talk about "cyberwar," but there may not be a war. If a victor can extract tribute from the vanquished, war isn't necessary. Today, intellectual capital is a proxy for tribute. We'll look at some specifics, including documents that outline the plan of attack, details about what operations have been run against us, and progress in efforts to create an international legal framework for when the bits start flying.

A Beginner's Guide to Cryptography Through Python *Kevin Fiscus*

Symmetric, asymmetric, message digest, substitution, transposition - these are cryptographic concepts that may be new to some people. Others may understand what they are but not how they work. This talk will provide an introduction to cryptographic topics using the Python programming language but will do so in a way that does not require you to be a cryptographer or a programmer. We will look at basic encryption techniques by creating simple programs in Python that put these techniques into practice. We will also look at some basic attacks against encryption also using Python. If you are new to security and want to learn about encryption, this presentation is for you. If you have a decent understanding of the terms associated with cryptography but want to understand a little more about the mechanics involved, this presentation is for you. If you understand encryption and want to get some exposure to Python, this presentation is for you.

GIAC Program Overview

SANS Technology Institute Open House

What's Your Next Career Move?

The information security field is growing and maturing rapidly.
Are you positioned to grow with it?
A Master's Degree in Information Security from the
SANS Technology Institute (STI) will help you build knowledge
and skills in management or technical engineering.

The SANS Technology Institute (STI) offers two unique master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

"The STI program prepares me in both technical aptitude and leadership skills. The instructors have extensive real-world experience - you walk out of every class with skills you can use immediately."

-Courtney Imbert, MSISE Student

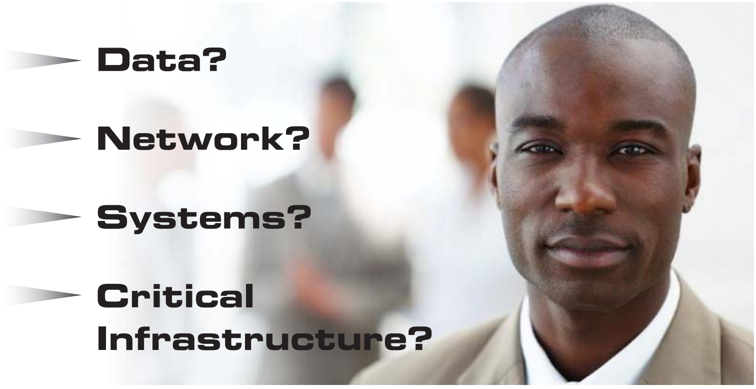
Apply today for the Fall 2013 cohort!

www.sans.edu

SANS Technology Institute
Knowledge for Peace
Scientia Pro Pace

www.sans.edu
info@sans.edu
855-672-6733

How Are You Protecting Your



- Data?
- Network?
- Systems?
- Critical Infrastructure?

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size-fits-all security certification.
Get GIAC certified!

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

"GIAC is the only certification that proves you have hands-on technical skills."
-Christina Ford, Department of Commerce

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-Alan C, USMC

Get Certified at
www.giac.org

Department of Defense Directive 8570 *(DoD 8570)*

www.sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct information assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC provides the most options in the industry for meeting 8570 requirements.

SANS Training Courses for DoD Approved Certifications

SANS TRAINING COURSE		DoD APPROVED CERT
SEC401	Security Essentials Bootcamp Style	**GSEC**
SEC503	Intrusion Detection In-Depth	**GCIA**
SEC504	Hacker Techniques, Exploits & Incident Handling	**GCIH**
AUD507	Auditing Networks, Perimeters, and Systems	**GSNA**
MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	**CISSP**
MGT512	SANS Security Essentials for Managers with Knowledge Compression™	**GSLC**

Compliance/Recertification:

To stay compliant with DoD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years. Go to www.giac.org to learn more about certification renewal.

DoD 8570 certification requirements are subject to change, please visit http://iase.disa.mil/eta/iawip for the most updated version.

For more information, contact us at 8570@sans.org or visit www.sans.org/8570

SECURITY AWARENESS

FOR THE 21st CENTURY

- Go beyond compliance and focus on changing behaviors.
- Training is mapped against the 20 Critical Controls framework.
- Create your own program by choosing a variety of End User awareness modules.
- Enhance training by adding compliance topics, such as NERC-CIP, PCI DSS, HIPPA, FERPA, and Red Flags, to name a few.
- Test your employees and identify vulnerabilities through phishing emails.
- For a free trial visit us at www.securingthehuman.org

www.securingthehuman.org

Future SANS Training Events

SANS Rocky Mountain 2013

Denver, CO | July 14-20

www.sans.org/event/rocky-mountain-2013

SANS San Francisco 2013

San Francisco, CA | July 29 - August 3

www.sans.org/event/san-francisco-2013

SANS Boston 2013

Boston, MA | August 5-10

www.sans.org/event/boston-2013

SANS Virginia Beach 2013

Virginia Beach, VA | August 19-30

www.sans.org/event/virginia-beach-2013

SANS Network Security 2013

Las Vegas, NV | September 14-23

www.sans.org/event/network-security-2013

SANS Seattle 2013

Seattle, WA | October 7-12

www.sans.org/event/seattle-2013

SANS Chicago 2013

Chicago, IL | Oct 28 - Nov 2

www.sans.org/event/chicago-2013

SANS South Florida 2013

Fort Lauderdale, FL | November 4-9

www.sans.org/event/sans-south-florida-2013

SANS Training Formats

LIVE CLASSROOM TRAINING

Multi-Course Training Events

Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking with your peers

www.sans.org/security-training/bylocation/index_all.php

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

www.sans.org/community

OnSite

Live Training at Your Office Location

www.sans.org/onsite

Mentor

Live Multi-Week Training with a Mentor

www.sans.org/mentor

Summit

Live IT Security Summits and Training

www.sans.org/summit

ONLINE TRAINING

OnDemand

E-Learning available anytime, anywhere, at your pace

www.sans.org/ondemand

vLive

Live, Online Instruction from SANS' Top Instructors

www.sans.org/vlive

Simulcast

Attend a SANS Training Event Without Leaving Home

www.sans.org/simulcast

CyberCon

Live Online Training Event

www.sans.org/event/cybercon-fall-2013

SelfStudy

Books and MP3 Files for Independent Learners

www.sans.org/selfstudy

SANS Capital City 2013

Hotel Information

Training Campus
Grand Hyatt Washington

1000 H Street NW | Washington, DC 20001
Phone: 202-582-1234
www.sans.org/event/sans-capital-city-2013/location

Special Hotel Rates Available

A special discounted rate of $189.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID but the specially negotiated SANS rate is lower; 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 August 12, 2013.

Experience the upscale elegance of Grand Hyatt Washington, a full-service Washington, DC hotel. Centrally located in the trendy Penn Quarter near popular local attractions, the hotel is ideally situated for leisure and business travelers. Grand Hyatt Washington is a welcoming destination with a host of world-class services and amenities.

Top 5 reasons to stay at the Grand Hyatt Washington

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 Grand Hyatt Washington, 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 Grand Hyatt Washington that you won't want to miss!

5 Everything is in one convenient location!

SANS Capital City 2013

Registration Information

SANS
The Most Trusted Source for Information and Software Security Training

We recommend you register early to ensure you get your first choice of courses.
Register online at www.sans.org/event/sans-capital-city-2013

To register, go to
www.sans.org/event/sans-capital-city-2013

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

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

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

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

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 August 7, 2013 – processing fees may apply.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	7/24/13	$500.00	8/7/13	$250.00

Some restrictions apply.

Group Savings (Applies to tuition only)

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

To obtain a group discount, complete the discount code request form at **www.sans.org/security-training/discounts** prior to registering.

SANS Voucher Credit Program

Expand your Training Budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
www.sans.org/vouchers