

# SANS

THE MOST TRUSTED NAME IN HANDS-ON  
INFORMATION & SOFTWARE SECURITY  
TRAINING & PROFESSIONAL CERTIFICATION

## Community SANS in East Africa

NAIROBI, KENYA

# 2011

### SEC401: SANS Security Essentials Bootcamp Style

23-28 MAY, 2011

### FOR408: Computer Forensic Investigations - Windows In-Depth

6-11 JUNE, 2011



*"The perfect balance of theory and hands-on experience."*

—JAMES D. PERRY II, UNIVERSITY OF TENNESSEE



# SEC401: SANS Security Essentials Bootcamp Style

MONDAY MAY, 23–SATURDAY MAY, 28

INSTRUCTOR : JOHNNY LONG | 6-DAY COURSE | 46 CPE CREDITS | LAPTOP REQUIRED

## course overview

Maximize your training time and turbo-charge your career in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification. In this course you will learn the language and underlying theory of computer security. At the same time you will learn the essential, up-to-the-minute knowledge and skills required for effective performance 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 up-to-the-minute 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. As always, great teaching sets SANS courses apart, and SANS ensures this by choosing instructors who have ranked highest in a nine-year competition among potential security faculty.

*“SANS gives real world examples of tools and how to use them.”*

—NICHOLE KENNEDY, OKDOC



Get GSEC Certified  
<http://www.giac.org>

## course description

### DAY 1: NETWORKING CONCEPTS

A key way attackers gain access to a company's resources is through a network connected to the Internet. A company wants to try to prevent as many attacks as possible; but in cases where it cannot prevent an attack, it must detect it in a timely manner. Therefore, an understanding of how networks and the related protocols like TCP/IP work is critical to being able to analyze network traffic and determine hostile traffic. It is just as important to know how to protect against these attacks using devices such as routers and firewalls. These essentials, and more, will be covered to provide a firm foundation for the consecutive days training.

### DAY 2: DEFENSE IN-DEPTH

In order to secure an enterprise network, you must have an understanding of the general principles of network security. In this course, you will learn about six key areas of network security. The day starts with information assurance foundations, where students look at both current and historical computer security threats, and how they have impacted confidentiality, integrity and availability. The first half of the day also covers the instruction for creating sound security policies and password management, including tools for password strengths on both Unix and Windows platforms. The second half of the day is spent on understanding the information warfare threat and the six steps of incident handling. The day draws to a close by looking at what can be done to test and protect a web server in your company.

### DAY 3: INTERNET SECURITY TECHNOLOGIES

Military agencies, banks and retailers offering electronic commerce programs, and dozens of other types of organizations are demanding to know what threats they are facing and what they can do to alleviate those threats. In this course, you will obtain a roadmap that will help you understand the paths available to organizations that are considering or planning to deploy various security devices and tools such as intrusion detection systems and firewalls. The course goes beyond the narrow technical view and offers a full context for the deployment of these promising new technologies. When it comes to securing your enterprise,

there is no single technology that is going to solve all of a company's security issues. However, by implementing an in-depth defense strategy that includes multiple defensive measures, you can go a long way in securing your enterprise. Each section in this course covers one tool that will play a part in a company's overall information assurance program.

### DAY 4: SECURE COMMUNICATIONS

There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, though few companies use it. This technology is encryption. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. Day 4 looks at various aspects of encryption and how it can be used to secure a company's assets. A related area called steganography, or information hiding, is also covered. Wireless is becoming a part of most modern networks but they are often implemented in a non-secure manner. Security issues associated with wireless and what can be done to protect these networks will also be discussed. This section finishes by tying all of the other pieces together by looking at Operations Security.

### DAY 5: WINDOWS SECURITY

Windows is the most widely-used and hacked operating system on the planet. At the same time, the complexities of Active Directory, PKI, BitLocker, AppLocker and User Account Control represent both challenges and opportunities. This section will help you to quickly master the world of Windows security while showing you the tools you can use to simplify and automate your work. You will complete the day with a solid grounding in Windows security, including the important new features in Windows 7 and Server 2008-R2.

### DAY 6: LINUX SECURITY

Based on industry consensus standards, this course provides step-by-step guidance on improving the security of any Linux system. The course combines practical "how to" instructions with background information for Linux beginners and security advice and "best practices" for administrators of all levels of expertise.

# FOR408:

## Computer Forensic Investigations - Windows In-Depth

**MONDAY JUNE, 6-SATURDAY JUNE, 11**

**INSTRUCTOR : ISMAEL VALENZUELA | 6-DAY COURSE | 36 CPE CREDITS | LAPTOP REQUIRED**

### who should attend

- » Information technology professionals who wish to learn the core concepts in computer forensics investigations
- » Incident Response Team Members who are responding to security incidents and need to utilize computer forensics to help solve their cases
- » Law enforcement officers, federal agents, or detectives who desire to become a subject matter expert on computer forensics for Windows based operating systems
- » Information security managers who need to understand digital forensics in order to understand information security implications and potential litigation related issues or manage investigative teams
- » Information technology lawyers and paralegals who desire to have a formal education in digital forensic investigations
- » Anyone interested in computer forensic investigations with a background in information systems, information security, and computers

### sampling of topics

- » Digital Forensics Essentials
- » Windows File System Basics
- » Fundamental Forensic Methodology
- » Evidence Acquisition Tools and Techniques
- » Law Enforcement Bag and Tag
- » Evidence Integrity
- » Presentation and Reporting of Evidence and Analysis
- » Windows XP, VISTA, and Windows 7 Investigation and Analysis
- » Windows In-Depth Registry Forensics
- » Tracking User Activity
- » And Much More...



Get GCFE Certified  
<http://www.giac.org>

***Fight crime. Unravel incidents... one byte at a time!***

## course overview

This course focuses on the critical knowledge that a computer forensics investigator must know to investigate computer crime incidents successfully. You will learn how computer forensics analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation. This course covers the fundamental steps of the in-depth computer forensics methodology so that each student will have the complete qualifications to work as a computer forensics investigator in the field helping solve and fight crime. In addition to in-depth technical digital forensics, knowledge on Windows Digital Forensics (Windows XP through Windows 7 and Server 2008) you will be exposed to well known computer forensics tools so such as FTK, Registry Analyzers, FTK Imager, Prefetch Analyzers, and much more.

## course description

### **DAY 1: DIGITAL FORENSICS AND E-DISCOVERY FUNDAMENTALS**

**FOCUS:** Investigations begin with a firm knowledge in proper evidence acquisition and analysis. Digital Forensics is more than just using a tool that automatically recovers data. You must focus on the facts to seek the truth. Digital Forensics requires analytical skills. Today you will learn how the professionals accomplish digital forensics.

### **DAY 2: EVIDENCE ACQUISITION AND ANALYSIS**

**FOCUS:** You will learn proper evidence acquisition, integrity, and handling skills of logical, physical, and system memory utilizing the Tableau T35es writer. Moving quickly from acquisition, you will begin your investigation using cutting-edge tools that the pros use.

### **DAY 3: CORE WINDOWS FORENSICS PART I - EMAIL AND REGISTRY ANALYSIS**

**FOCUS:** Beginning with host, server, and webmail forensics the investigator will learn how to recover and analyze the most world's most popular form of communication. Following this, the next focus centers on Windows XP, Vista, and Windows 7 Registry Analysis and USB Device Forensics.

### **DAY 4: CORE WINDOWS FORENSICS PART II - ARTIFACT AND BROWSER FORENSICS**

**FOCUS:** Hundreds of files are created by actions of the suspect. Learn how to examine key files such as link files, the windows prefetch, pagefile/system memory, and more. Internet Explorer and Firefox Browser Digital Forensics is covered in detail. Learn how to examine exactly what an individual did while surfing via their web-browser. The results will give you pause the next time you use the web.

### **DAY 5: CORE WINDOWS FORENSICS PART III - WEB BROWSER FORENSICS**

**FOCUS:** Windows Vista/7 Based Digital Forensic Challenge. There has been a murder-suicide and you have been called in to investigate the system. This day is a capstone for every artifact discussed in the class. You will use this day to solidify your skills that you have learned over the past week.

### **DAY 6: DIGITAL FORENSIC CHALLENGE AND MOCK TRIAL**

**FOCUS:** Windows Vista/7 Based Digital Forensic Challenge. There has been a murder-suicide and you have been called in to investigate the system. This day is a capstone for every artifact discussed in the class. You will use this day to solidify your skills that you have learned over the past week.

# training venue

## Nairobi Safari Club - Lillian Towers

Koinange Street / University Way Nairobi, Kenya

Tel: +254-20-2821000 • Fax: +254-20-2215137

info@nairobisafariclub.com | <http://www.nairobisafariclub.com>



# registration information

**DETAIL & REGISTRATION:** <http://www.sans.org/east-africa-2011-cs/>

**TUITION:** **SEC401: SANS Security Essentials Bootcamp Style = \$3,750**

add Proctored GSEC \$499 | add OnDemand \$399

**FOR408: Computer Forensics Investigations - Windows In-Depth = \$3,750**

add Proctored GCFE \$499 | add OnDemand \$399

**SANS CONTACT:** Barbara Basalgete, Director SANS EMEA: +44 20 3384 3473 | [bbasalgete@sans.org](mailto:bbasalgete@sans.org)

**K-NINETY CONTACT:** Preston Odera, CEO: +254 722 771478 | [preston.oder@gmail.com](mailto:preston.oder@gmail.com)

# about the instructors



**JOHNNY LONG**  
— INSTRUCTOR —

Johnny Long is the founder of Hackers For Charity (HFC) an organization that seeks to connect the skills of the hacker community with charities like AOET that need those skills. HFC seeks to empower the world's most vulnerable citizens while providing positive outlets for hackers and providing them

referrals to help secure work they are passionate about.

<http://www.hackersforcharity.org>



**ISMAEL VALENZUELA**  
— INSTRUCTOR —

Since he founded one of the first IT Security consultancies in Spain, Ismael Valenzuela has participated as a security professional in numerous international projects across EMEA, India and Australia in the last 10 years. He currently works as Global IT Security Manager for iSOFT Group Ltd. Ismael's expertise includes security assessments, penetration testing, risk analysis, ISO 27001 implementation, security architecture design and review, IDS/IPS technology, traffic analysis, log correlation, incident handling and digital forensic analysis. Ismael also serves on

the GIAC Advisory Board, and is an international instructor for the British Standard Institute (BSI). Ismael has also authored several articles on a wide range of security topics. Some of his articles are freely available at <http://blog.ismaelvalenzuela.com> and can be followed on twitter at <http://twitter.com/aboutsecurity>.

## about the Community SANS program in EMEA

The Community SANS format in EMEA (Europe, Middle East and Africa Region) offers the most popular SANS courses in your local community and in your local language. The classroom setting is small with fewer than 25 students. The instructors are pulled from the best of the local mentor program or qualified security experts who have passed SANS rigorous screening process called "the murder boards". The course material is delivered over consecutive days, and the course content is the same as ones provided at a larger training event. In addition to the excellent courseware, not only will you be able to use the skills that you learned as soon as you return to the office, but you will be able to continue to network with colleagues in your community that you meet at the training.

**SANS has partnered with K-Ninety East Africa Ltd. to bring the SEC401 & FOR408 courses for the first time to East Africa. K-Ninety will be promoting the event locally.**

## about SANS

SANS is the most trusted and by far the largest source for training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the

challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.

<http://www.sans.org>

## about K-Ninety East Africa Ltd.

K-Ninety East Africa Ltd. (K-90) is a consulting company dealing in training, conferences, e-learning solutions, bandwidth optimization solutions, IS audit, forensics audit, information systems security, and computer audit solution.

<http://k-90ea.com>