SANS

The Most Trusted Name in Hands-on Information & Software Security Training & Professional Certification

Community SANS Madrid

September 20–29 2012

SEC503:
Intrusion Detection In-Depth

SEC560:
Network Penetration Testing and Ethical Hacking

"I have attended many conferences & training sessions, and SANS by far has been the best. The instructors are the top in the industry, examples are from real life experiences – terrific!"

–CHRIS BUSH, NOVARTIS PHARMACEUTICALS

VASS

SANS Community

SEC503 Intrusion Detection In-Depth

THU. SEPTEMBER 20, 2012 -> SAT. SEPTEMBER 29, 2012

ISMAEL VALENZUELA, INSTRUCTOR

6-DAY COURSE | 9:00 AM–5:00 PM | 36 CPE/CMU CREDITS | LAPTOP REQUIRED

Get GCIA certified HTTP://WWW.GIAC.ORG

Days 1-3 of the course will take place from 20-22 September and Days 4-6 of the courses will take place from 27-29 September. This course will be taught in Spanish, but coursebooks will be in English.

course overview

Learn practical hands-on intrusion detection and traffic analysis from top practitioners/authors in the field. This challenging track methodically progresses from understanding the theory of TCP/IP, examining packets, using Snort to analyze traffic, becoming familiar with the tools and techniques for traffic and intrusion analysis, to reinforcing what you've learned with a hands-on challenge of investigating an incident. Students should be able to "hit the ground running" once returning to a live environment where traffic analysis it required.

This is a fast-paced course, and students are expected to have a basic working knowledge of TCP/IP in order to fully understand the topics that will be discussed. Although others may benefit from this course, it is most appropriate for students who are or who will become intrusion detection/prevention analysts. Students generally range from novices with some TCP/IP background all the way to seasoned analysts. The challenging hands-on exercises are specially designed to be valuable for all experience levels. We strongly recommend that you spend some time getting familiar with tcpdump before coming to class.

who should attend

Intrusion detection analysts (all levels)

Network engineers

System, security, and network administrators

Hands-on security managers

prerequisite

Students must possess at least a working knowledge of TCP/IP and hexadecimal. To test your knowledge, see our TCP/IP & Hex Quizzes at *http://www.sans.org/security-training/tcpip_quiz.php*

sample of topics

TCP/IP

- Tcpdump Overview and TCP/IP concepts
- ICMP
- Fragmentation
- Stimulus - Response
- Microsoft Protocols
- Domain Name System (DNS)
- IPv6

HANDS-ON TCPDUMP ANALYSIS

- Mechanics of running tcpdump
- General network traffic analysis

HANDS-ON SNORT USAGE

- Various modes of running Snort
- Writing Snort rules

INTRUSION ANALYSIS

- Intrusion Detection Architecture
- Intrusion Detection/Prevention Analysis

"This was by far the best course I have ever taken."

–PETER LOMBARS, INTRUCOM INC.

author statement

When I was invited to be a member of a computer incident response team in the late 1990's (just after Al Gore invented the Internet), there was no formal cybersecurity training available. Consequently, I learned on the job and made my share, and then some, of mistakes. I was so naive that I tried to report an attack on our network by a host with an IP address in the 192.168 reserved private network, available for use by anyone. Needless to say, I got a very embarrassing enlightenment when someone clued me in.

With the benefit of experience and the passage of time, there are many lessons to be shared with you. This knowledge affords you the opportunity to learn and practice in the classroom to prepare you for the fast-paced always-interesting job of intrusion detection analysts. ***–Judy Novak***

SEC560

THU. SEPTEMBER 20, 2012
-> SAT. SEPTEMBER 29, 2012

Network Penetration Testing and Ethical hacking

Get GPEN certified
HTTP://WWW.GIAC.ORG

JOSE SELVI, INSTRUCTOR
6-DAY COURSE | 9:00 AM–5:00 PM | 36 CPE/CMU CREDITS | LAPTOP REQUIRED

Days 1-3 of the course will take place from 20-22 Sept. and Days 4-6 will take place from 27-29 Sept. This course will be taught in Spanish, but coursebooks will be in English.

course overview

Equipping Security Organizations with Advanced Penetration Testing and Ethical Hacking Know-How

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from our infrastructures. Lots of people claim to have penetration testing, ethical hacking, and security assessment skills, but precious few can apply these skills in a methodical regimen of professional testing to help make an organization more secure. This class covers the ingredients for successful network penetration testing to help attendees improve their enterprise's security stance.

We address detailed pre-test planning, including setting up an effective penetration testing infrastructure and establishing ground rules with the target organization to avoid surprises and misunderstanding. Then, we discuss a time-tested methodology for penetration and ethical hacking across the network, evaluating the security of network services and the operating systems behind them.

Attendees will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, and social networking sites. We'll then turn our attention to scanning, experimenting with numerous tools in hands-on exercises. Our exploitation phase will include the use of exploitation frameworks, stand-alone exploits, and other valuable tactics, all with hands-on exercises in our lab environment. The class also discusses how to prepare a final report, tailored to maximize the value of the test from both a management and technical perspective. The final portion of the class includes a comprehensive hands-on exercise, conducting a penetration test against a hypothetical target organization, following all of the steps.

The course also describes the limitations of penetration testing techniques and other practices that can be used to augment penetration testing to find vulnerabilities in architecture, policies, and processes. We also address how penetration testing should be integrated as a piece of a comprehensive enterprise information security program.

why choose SANS' ethical hacking course for your pen testing needs?

This SANS course differs from other penetration testing and ethical hacking courses in several important ways:

- We get deep into the tools arsenal with numerous hands-on exercises that show subtle, less-well-known, and undocumented features that are incredibly useful for professional penetration testers and ethical hackers.
- The course discusses how the tools interrelate with each other in an overall testing process. Rather than just throwing up a bunch of tools and playing with them, we analyze how to leverage information from one tool to get the most bang out of the next tool.
- We focus on the workflow of professional penetration testers and ethical hackers, proceeding step-by-step discussing the most effective means for conducting projects.
- The sessions address common pitfalls that arise in penetration tests and ethical hacking projects, providing real-world strategies and tactics for avoiding these problems to maximize the quality of test results.
- We cover several timesaving tactics based on years of in-the-trenches experience from real penetration testers and ethical hackers, actions that might take hours or days unless you know the little secrets we'll cover that will let you surmount a problem in minutes.
- The course stresses the mind-set of successful penetration testers and ethical hackers, which involves balancing the often contravening forces of creative "outside-the-box" thinking, methodical trouble-shooting, carefully weighing risks, following a time-tested process, painstakingly documenting results, and creating a high quality final report that achieves management and technical buy-in.
- We also analyze how penetration testing and ethical hacking should fit into a comprehensive enterprise information security program.

author statement

Successful penetration testers don't just throw a bunch of hacks against an organization and regurgitate the output of their tools. Instead, they need to understand how these tools work indepth, and conduct their test in a careful, professional manner. This course explains the inner workings of numerous tools and their use in effective network penetration testing and ethical hacking projects. When teaching the class, I particularly enjoy the numerous hands-on exercises culminated with a final pen-testing extravaganza lab. ***–Ed Skoudis***

about the instructors

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 11 years. He currently works as Principal Architect at McAfee (Foundstone Professional Services) where he delivers high quality security consultancy and training on a wide variety of topics, including security assessments, penetration testing, risk analysis, ISO/IEC 27001 implementation, security architecture design and review, IDS/IPS technology, traffic analysis, log correlation, incident handling and digital forensic analysis. Prior to joining Foundstone, Ismael worked as Global IT Security Manager for iSOFT Group Ltd, one of the world's largest providers of healthcare IT solutions, focusing on establishing and managing the IT Security program in more than 40 countries while providing risk-driven strategic planning, defining an ISO 27001 compliant policy framework and working with the applications team to ensure that security was embedded into their SDLC. Author of security articles for Hakin9, INSECURE Magazine and the SANS Forensics Blog, Ismael also serves on the GIAC Advisory Board and is a Community SANS Instructor for the Computer Forensics and Intrusion Detection tracks. He holds a bachelor's degree in computer science from the University of Malaga (Spain), is certified in Business Administration, and holds several professional certifications including GREM, GCFA, GCIA, GCIH, GPEN, GCUX, GCWN, GWAPT, GSNA, CISSP, ITIL, CISM and IRCA 27001 Lead Auditor from Bureau Veritas UK. Some of his articles are freely available at his http://blog.ismaelvalenzuela.com (his information security blog). Mr. Valenzuela can be followed on twitter at @aboutsecurity.

JOSE SELVI
— INSTRUCTOR —

Jose Selvi is currently a Pentester at S21sec, an important Security Company in Spain. In the past, he worked for Telefonica (ISP), Panda Security (AV) and local government in Spain. In the last seven years, Jose has been concentrating mainly on Penetration Testing, Intrusion Detection, Incident Handling and Forensics. Jose has a Master Degree in Computer Science and a Bachelor Degree in Telecommunications. He is also currently preparing a security-related PhD Thesis, and holds the CISA, CISSP, CNAP, GCIH and GPEN certifications.

training venue

VASS Consultoría de Sistemas
Avda. Doctor Severo Ochoa, 25 - 1ª Planta • 28100 Alcobendas (Madrid)
http://www.vass.es

registration information

DETAIL & REGISTRATION:
http://www.sans.org/info/1065792
http://www.sans.org/info/106584

SEC503: Intrusion Detection in-Depth = €3150
Discount if paid by August 22, 2012 = €200 | Discount if paid by August 8, 2012 = €300
=> Add Proctored GCIA €499 | Add €399 for OnDemand

SEC560: Network Penetration Testing and Ethical Hacking = €3150
Discount if paid by August 22, 2012 = €200 | Discount if paid by August 8, 2012 = €300
=> Add Proctored GPEN €499 | Add €399 for OnDemand

All amounts listed are in euros • Refund deadline: August 29, 2012

contact information

CONTACT @ SANS: Barbara Basalgète, SANS EMEA Director: +33 6 71 48 24 01 | bbasalgete@sans.org

CONTACT @ VASS: Marlene Sánchez: +34 91 662 34 04 | marlene.sanchez@vass.es
Rafael Ausejo Prieto: rafael.ausejo@vass.es

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.

VASS has partnered with SANS to bring the SEC503 and SEC560 courses to Spain for the first time in the Community SANS format.

About SANS

SANS is the most trusted and by far the largest source for information security training and certi!cation 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. SANS provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited. Courses address both security fundamentals and awareness and the in-depth technical aspects of the most crucial areas of IT security.

http://www.sans.org

About VASS

VASS is an IT consulting firm highly specialized in new technologies and product and service integration with a profound technical knowledge and control. VASS is a 100% private and independent company, with a high level of expertise and innovation. Its offices in Madrid, Barcelona and London, have the capacity to provide services all over the European territory through local alliances and by displacing its resources according to customers requirements.

Since 1999, VASS' strategy has been to select those business areas of strategic value (CRM, eBusiness, Business Intelligence, Microsoft, ERP, Innovation, Security and System Operation Information) betting on each of the technologies that we believe are the market leaders and drivers. Building on these technologies, highly specialized teams provide the market with a successful model combination: agility, flexibility with deep knowledge of the technology involved. **http://www.vass.es**