Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

ECSA - EC Council Certified Security Analyst

Course Description

SecureNinja's EC Council Certified Security Analyst, ECSA training and certification boot camp is an advanced ethical hacking training certification that complements the CEH (Certified Ethical Hacker) certification by exploring the analytical phase of ethical hacking. This boot camp is also taught by our very own ninja instructors available in Washington DC, San Diego CA, and Live Online. While the Certified Ethical Hacker certification exposes the learner to hacking tools and technologies, the Certified Security Analyst course takes it a step further by exploring how to analyze the outcome from these tools and technologies. Through groundbreaking network penetration testing methods and techniques, this pen testing computer security certification helps students perform the intensive assessments required to effectively identify and mitigate risks to the information security of the infrastructure.

This makes the Certified Security Analyst "Pen Testing" certification a relevant milestone toward achieving EC Council's Licensed Penetration Tester, which also ingrains the learner in the business aspect of network penetration testing. The Licensed Penetration Tester standardizes the knowledge base for network penetration testing professionals by incorporating the best practices followed by experienced experts in the field.

The objective of Certified Security Analyst "pen testing" certification is to add value to experienced Information security professionals by providing computer security training that will help them analyze the outcomes of their Vulnerability Assessments. Network Penetration Testing Training leads the learner into the advanced stages of ethical hacking.

Advanced Penetration Testing and Security Analysis
The Certified Security Analyst "pen testing" program is a computer security certification designed to teach Information Security Professionals the advanced uses of the available methodologies, tools, and techniques expected from a premier ethical hacking training and are required to perform comprehensive information security pen tests. Students will learn how to design, secure and test networks to protect your organization from the threats hackers and crackers pose. By teaching the Licensed Penetration Tester, LPT methodology and groundbreaking techniques for security and penetration testing, this class will help you perform the intensive assessments required to effectively identify and mitigate risks to the security of your infrastructure. As students learn to identify Information Security problems in this ethical hacking training certification course, they also learn how to avoid and eliminate them, with the class by providing complete coverage of analysis and network security-testing topics.

Topics Covered

- The Need for Security Analysis
- Advanced Googling
- TCP/IP Packet Analysis

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Advanced Sniffing Techniques
- Vulnerability Analysis with Nessus
- Advanced Wireless Testing
- Designing a DMZ
- Snort Analysis
- Log Analysis
- Advanced Exploits and Tools
- Pen Testing Methodologies
- Customers and Legal Agreements
- Rules of Engagement
- Penetration Testing Planning and Scheduling
- Pre Penetration Testing Checklist
- Information Gathering
- Vulnerability Analysis
- External Penetration Testing
- Internal Network Penetration Testing
- Routers and Switches Penetration Testing
- Firewall Penetration Testing
- IDS Penetration Testing
- Wireless Network Penetration Testing
- Denial of Service Penetration Testing
- Password Cracking Penetration Testing
- Social Engineering Penetration Testing
- Stolen Laptop, PDAs and Cell phones Penetration Testing
- Application Penetration Testing
- Physical Security Penetration Testing
- Database Penetration testing
- VoIP Penetration Testing
- VPN Penetration Testing
- War Dialing
- Virus and Trojan Detection
- Log Management Penetration Testing
- File Integrity Checking
- Blue Tooth and Handheld Device Penetration Testing
- Telecommunication and Broadband Communication Penetration Testing
- Email Security Penetration Testing
- Security Patches Penetration Testing
- Data Leakage Penetration Testing
- Penetration Testing Deliverables and Conclusion
- Penetration Testing Report and Documentation Writing
- Penetration Testing Report Analysis
- Post Testing Actions
- Ethics of a Licensed Penetration Tester
- Standards and Compliance

Requirements

Before a candidate can sit for the ECSA exam, they must attend, and complete, EC Council official training. SecureNinja is an official EC Council Accredited Training Center and all students who complete our ECSA boot camp will qualify.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Course Benefits

- ECSA is for experienced hands in the industry and is backed by a curriculum designed by the best in the field.
- Greater industry acceptance as a seasoned security professional.
- Learn to analyze the outcomes of using security tools and security testing techniques.
- A requirement for the LPT certification

Certification Exam

Students will be prepared for EC-Council's ECSA v10 on the last day of the class. This certification is also pre-requisite to EC-Council's Licensed Penetration Tester Program.

Who Should Attend

Network server administrators, Firewall Administrators, Information Security Testers, System Administrators and Risk Assessment Professionals.

Why Get This Advanced Ethical Hacking / Penetration Tester Certification?

Computers around the world are systematically being victimized by rampant hacking. This hacking is not only widespread but is being executed so flawlessly that the attackers compromise a system, steal everything of value and completely erase their tracks within 20 minutes.

Course Length

40 Hours

Follow-on Courses

The Licensed Penetration Tester (LPT); Network Penetration Testing