

<b>Acronym/Nickname</b> ECSA		<b>Certification Body</b> EC-COUNCIL	
<b>Description</b>  EC-Council Certified Security Analyst (ECSA) complements the Certified Ethical Hacker (CEH) certification by exploring the analytical phase of ethical hacking. While CEH exposes the learner to hacking tools and technologies, ECSA takes it a step further by exploring how to analyze the outcome from these tools and technologies. Through groundbreaking penetration testing methods and techniques, ECSA class helps students perform the intensive assessments required to effectively identify and mitigate risks to the security of the infrastructure.		<b>Certification Level</b> Professional  <b>Covered competencies</b> <ul style="list-style-type: none"> <li>Greater industry acceptance as seasoned security professional.</li> <li>Learn to analyze the outcomes from using security tools and security testing techniques.</li> </ul>	
		<b>Requirements</b>  Pass exam <b>412-79</b> to achieve EC-Council Certified Security Analyst (ECSA) certification	
<b>Target</b> Network server administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment professionals.		<b>Career Path</b>	
<b>Authorized Testing Center:</b>  PEARSON VUE / PROMETRIC	<b>Indicative Fee*</b>  300 USD	<b>Certification Schedule*</b>	
* Fees and schedules are subject to change without prior notice, please get in touch with certification body through contact details below			
<b>Recommended/Preparatory Training</b>  Module 1: The Need for Security Analysis Module 2: Advanced Googling Module 3: TCP/IP Packet Analysis Module 4: Advanced Sniffing Techniques Module 5: Vulnerability Analysis with Nessus Module 6: Advanced Wireless Testing Module 7: Designing a DMZ Module 8: Snort Analysis Module 9: Log Analysis Module 10: Advanced Exploits and Tools Module 11: Penetration Testing Methodologies Module 12: Customers and Legal Agreements Module 13: Penetration Testing Planning and Scheduling Module 14: Pre Penetration Testing Checklist Module 15: Information Gathering Module 16: Vulnerability Analysis Module 17: External Penetration Testing Module 18: Internal Network Penetration Testing Module 19: Router Penetration Testing Module 20: Firewall Penetration Testing Module 21: IDS Penetration Testing Module 22: Wireless Network Penetration Testing Module 23: Denial of Service Penetration Testing Module 24: Password Cracking Penetration Testing Module 25: Social Engineering Penetration Testing Module 26: Stolen Laptop Penetration Testing Module 27: Application Penetration Testing Module 28: Physical Security Penetration Testing Module 29: Database Penetration testing Module 30: VoIP Penetration Testing Module 31: VPN Penetration Testing Module 32: Penetration Testing Report Analysis Module 33: Penetration Testing Report and Documentation Writing Module 34: Penetration Testing Deliverables and Conclusion Module 35: Ethics of a Licensed Penetration Tester			
<b>Where to get more information:</b> <a href="http://www.eccouncil.org/ECSA.htm">http://www.eccouncil.org/ECSA.htm</a>			