

### Course Description |

ECSA/LPT is a security class like no other! Providing real world hands on experience, it is the only in-depth Advanced Hacking and Penetration Testing class available that covers testing in all modern infrastructures, operating systems and application environments. EC-Council's Certified Security Analyst/LPT program is a highly interactive 5-day security class designed to teach Security Professionals the advanced uses of the LPT methodologies, tools and techniques required to perform comprehensive information security 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 tools and ground breaking 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 security problems, they also learn how to avoid and eliminate them, with the class providing complete coverage of analysis and network security-testing topics.

### Course Outline |

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: Rules of Engagement  
Module 14: Penetration Testing Planning and Scheduling  
Module 15: Pre Penetration Testing Checklist  
Module 16: Information Gathering  
Module 17: Vulnerability Analysis  
Module 18: External Penetration Testing  
Module 19: Internal Network Penetration Testing  
Module 20: Routers and Switches Penetration Testing  
Module 21: Firewall Penetration Testing  
Module 22: IDS Penetration Testing  
Module 23: Wireless Network Penetration Testing  
Module 24: Denial of Service Penetration Testing  
Module 25: Password Cracking Penetration Testing  
Module 26: Social Engineering Penetration Testing  
Module 27: Stolen Laptop, PDAs and Cell phones Penetration Testing  
Module 28: Application Penetration Testing  
Module 29: Physical Security Penetration Testing  
Module 30: Database Penetration testing  
Module 31: VoIP Penetration Testing  
Module 32: VPN Penetration Testing  
Module 33: War Dialing  
Module 34: Virus and Trojan Detection  
Module 35: Log Management Penetration Testing  
Module 36: File Integrity Checking  
Module 37: Blue Tooth and Hand held Device Penetration Testing  
Module 38: Telecommunication and Broadband Communication Penetration Testing  
Module 39: Email Security Penetration Testing  
Module 40: Security Patches Penetration Testing  
Module 41: Data Leakage Penetration Testing  
Module 42: Penetration Testing Deliverables and Conclusion  
Module 43: Penetration Testing Report and Documentation Writing  
Module 44: Penetration Testing Report Analysis  
Module 45: Post Testing Actions  
Module 46: Ethics of a Licensed Penetration Tester  
Module 47: Standards and Compliance

### Who Should Attend |

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

### Duration |

5 days

### Exam |

The ECSA certification exam will be conducted on the last day of training. Students need to pass the online Prometric exam 412-79 to receive the ECSA certification. The Student also will be prepared for the LPT certification.

For more information please contact...



We know how to satisfy you!

**Vnohow (Thailand) Co., Ltd.**  
138 Boonmitr Building, 11th Floor,  
Room B1-B2, Silom Road,  
Suriyawong, Bangrak,  
Bangkok 10500 Thailand

Tel: +662-634-3287-89  
Fax: +662-634-3299  
Email: [vnohow@vnohow.com](mailto:vnohow@vnohow.com)  
Website: [www.vnohow.com](http://www.vnohow.com)

