EC-Council Security Analyst (ECSA)

Duration 5 Days

What's New in ECSA v10?

1. Maps to NICE 2.0 Framework
ECSAv10 maps to NICE framework's Analyze (AN) and Collect and Operate (CO) specialty area

2. ALL NEW Module for Social Engineering Pen Testing
The ECSA curriculum presents a comprehensive Social Engineering Pen Testing Methodology where others program only makes a mere reference of this. According to 2017 Verizon Data Breach Investigation Report, on an overall, 43% of the documented breaches involved social engineering attacks!

We see this as a huge gap and that is where, the ECSA program is carefully designed and developed to be comprehensive in its coverage of the pentesting domain.

3. Increased Focus on Methodologies
ECSA V10 brings an enhanced concentration on methodology for network, web application, database, wireless, and cloud pen testing, whereas other certifications cover this superficially.

The new ECSA v10 program takes the tools you have learnt in the CEH and includes a wide-range of comprehensive scoping and engagement penetration testing methodologies that improves upon the best from ISO 27001, OSSTMM, and NIST Standards.

4. Blended with both manual and automated penetration testing approach
There are many numbers of automated pen testing tools out there in the marketplace including high priced sophisticated tools, but they are not adequate. Most advanced tools are of little value if no one knows how to use them.

Manual penetration testing is the perfect complement to automated penetration Testing. Certain penetration test such as logic testing cannot be performed using automated tools. It requires human intervention to test against such vulnerabilities

According to the MITRE Corporation, automated pen testing tools cover only 45% of the known vulnerability types. Hence, the remaining 55% requires manual intervention.

5. Designed based on the most common penetration testing services provided by the penetration testing service providers and consulting firms in the market including:

- **Network Penetration Testing**
  Identify security issues in network design and implementation
- **Web Application Penetration Testing**
  Detect security issues in web applications that exists due to insecure design and development practices
- **Social Engineering Penetration Testing**
  Identify employees that do not properly authenticate, follow, validate, handle, the processes and technology
- **Wireless Penetration Testing**
  Identify misconfigurations in organization's wireless infrastructure including WLAN, Mobile,
- **Cloud Penetration Testing**
  Determine security issues in organization's cloud infrastructure
- **Database Penetration Testing**
  Identify security issues in the configuration of database server and their instances

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

WHO SHOULD ATTEND

Ethical Hackers, Penetration Testers, Security Analysts, Security Engineers, Network Server Administrators, Firewall Administrators, Security Testers, System Administrators, and Risk Assessment Professionals

CERTIFICATION

- **Credit Towards Certification:** ECSA v10
- **Number of Questions:** 150
- **Passing Score:** 70%
- **Test Duration:** 4 hours

OUTLINE

- **Module 01**: Introduction to Penetration Testing and Methodologies
- **Module 02**: Penetration Testing Scoping and Engagement Methodology
- **Module 03**: Open Source Intelligence (OSINT) Methodology
- **Module 04**: Social Engineering Penetration Testing Methodology
- **Module 05**: Network Penetration Testing Methodology - External
- **Module 06**: Network Penetration Testing Methodology - Internal
- **Module 07**: Network Penetration Testing Methodology - Perimeter Devices
- **Module 08**: Web Application Penetration Testing Methodology
- **Module 09**: Database Penetration Testing Methodology
- **Module 10**: Wireless Penetration Testing Methodology
- **Module 11**: Cloud Penetration Testing Methodology
- **Module 12**: Report Writing and Post Testing Actions

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th

Call us today 0-2634-7993-4

177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th