EC-Council

ECSA™

EC-Council Certified Security Analyst

v10

ANALYZE. SECURE. DEFEND.

Do you hold ECSA credential?

EC-Council Certified Security Analyst v10

EC-Council Certified Security Analyst (Practical)

EC-Council Security Analyst v10 (ECSA)

The ECSA program offers a seamless learning progress continuing where the CEH program left off.

The new ECSAv10 includes updated curricula and an industry recognized comprehensive step-by-step penetration testing methodology. This allows a learner to elevate their ability in applying new skills learned through intensive practical labs and challenges.

Unlike most other pen testing programs that only follow a generic kill chain methodology; the ECSA presents a set of distinguishable comprehensive methodologies that are able to cover different pentesting requirements across different verticals.

It is a highly interactive, comprehensive, standards based, intensive 5-days training program that teaches information security professionals how professional real-life penetration testing are conducted.

Building on the knowledge, skills and abilities covered in the new CEH v10 program, we have simultaneously re-engineered the ECSA program as a progression from the former.

Organizations today demand a professional level pentesting program and not just pentesting programs that provide training on how to hack through applications and networks.

Such professional level programs can only be achieved when the core of the curricula maps with and is compliant to government and/or industry published pentesting frameworks

This course is a part of the VAPT Track of EC-Council. This is a “Professional” level course, with the Certified Ethical Hacker being the “Core” and the Licensed Penetration Tester being the “Master” level certification.

In the new ECSAv10 course, students that passes the knowledge exam are given an option to pursue a fully practical exam that provides an avenue for them to test their skills, earning them the ECSA (Practical) credential. This new credential allows employers to validate easily the skills of the student.

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.

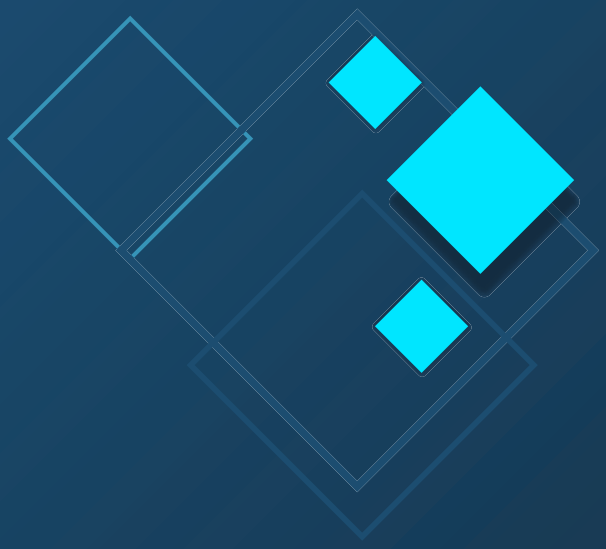
The new ECSA v10 program takes the tools you have learnt in the CEH and includes a wide-range of comprehensive scoping and engagement penetration testing methodologies that improves upon the best from ISO 27001, OSSTMM, and NIST Standards.

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.

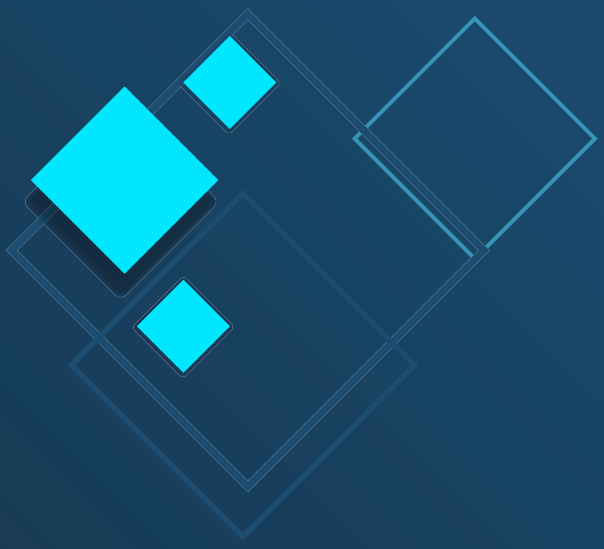


5. Designed based on the most common penetration testing services provided by the penetration testing service providers and consulting firms in the market including:

- **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

ECSA is the second step to achieve L|PT (Master) after C|EH and it is the most important step, you have to gather knowledge from C|EH and apply the same on E|CSA (Practical) and MCQ exam, E|CSA gave me the confidence to sit for a penetration testing on a live box, the courseware provided by EC-Council is as always great, filled with information and latest tools and techniques

- Agnidhra Chakraborty
(C|EH, ECSA, C|HFI, L|PT Master),
Co-Founder and CEO,
DFC Security



ECSA provides hands-on penetration testing experience. It covers the testing of infrastructures, operating systems and application environments and trains us on the process to document and write a penetration testing report. ECSA labs and challenges cover real-world scenario in penetration testing methodologies.

I recommend this course to anyone who wants to make a career in Information Security and to master Penetration Testing and Analysis.

- Feras M. Alzoubi,
Information Security Officer, Government

6. Presents a comprehensive scoping and engagement methodology

Defining scope of penetration test is arguably one of the most important components of a penetration test, yet it is also one of the most overlooked in most of the penetration testing programs. A complete module is dedicated in the course to describe the pre-engagement activities in detailed, tells how to initiate and set the scope and Rule of Engagement (RoE) for the penetration test assignment.

7. Provides strong reporting writing guidance to draft valuable and comprehensive penetration report

The report is the tangible output of the testing process, and the only real evidence that a test actually took place. Ultimately, it is the report that is sellable in penetration test assignment. If it is not well planned and drafted, the client may disagree with the findings of a test and will not justify the expense of the test. A separate module is dedicated in the course to describe the skills required to draft effective penetration test report depending upon the target audiences.

8. Hands-on labs demonstrating practical and real-time experience on each of area of penetration testing

Practical knowledge can lead to a deeper understanding of a concept through the act of doing. The course is also aiming to provide practical experience through hands-on labs on thorough penetration testing process from scoping and engagement to report writing The student will get a direct experience by working on these hands-on labs.

9. Provides standard templates that are required during penetration test

The course is bundled with the bunch of standard templates that are necessary which helps students during scoping and engagement process well as collecting and reporting test results. No other program offers a set of comprehensive penetration templates like the ECSA!

The EC-Council iLabs Cyber Range

The ECSA course is a fully hands-on program with labs and exercises that cover real world scenarios. By practicing the skills that are provided to you in the ECSA class, we are able to bring you up to speed with the skills to uncover the security threats that organizations are vulnerable to.

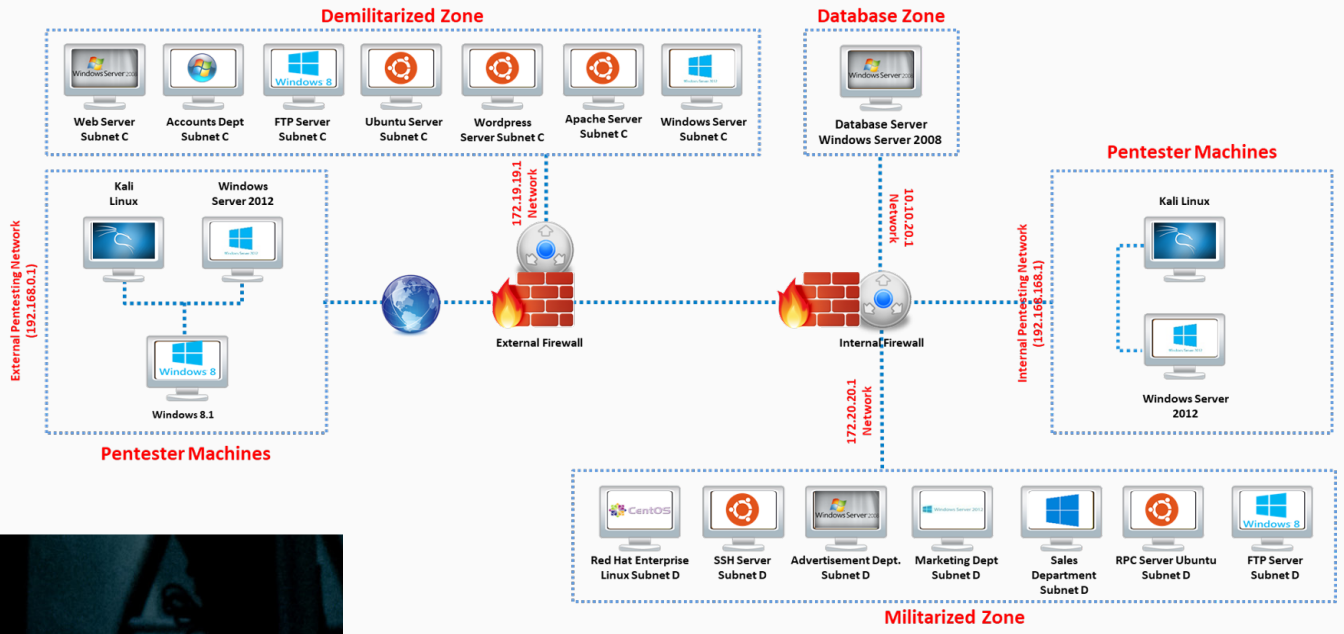
This can be achieved effectively with the EC-Council iLabs Cyber Range. It allows you to dynamically access a host of Virtual Machines preconfigured with vulnerabilities, exploits, tools, and scripts from anywhere with an internet connection.

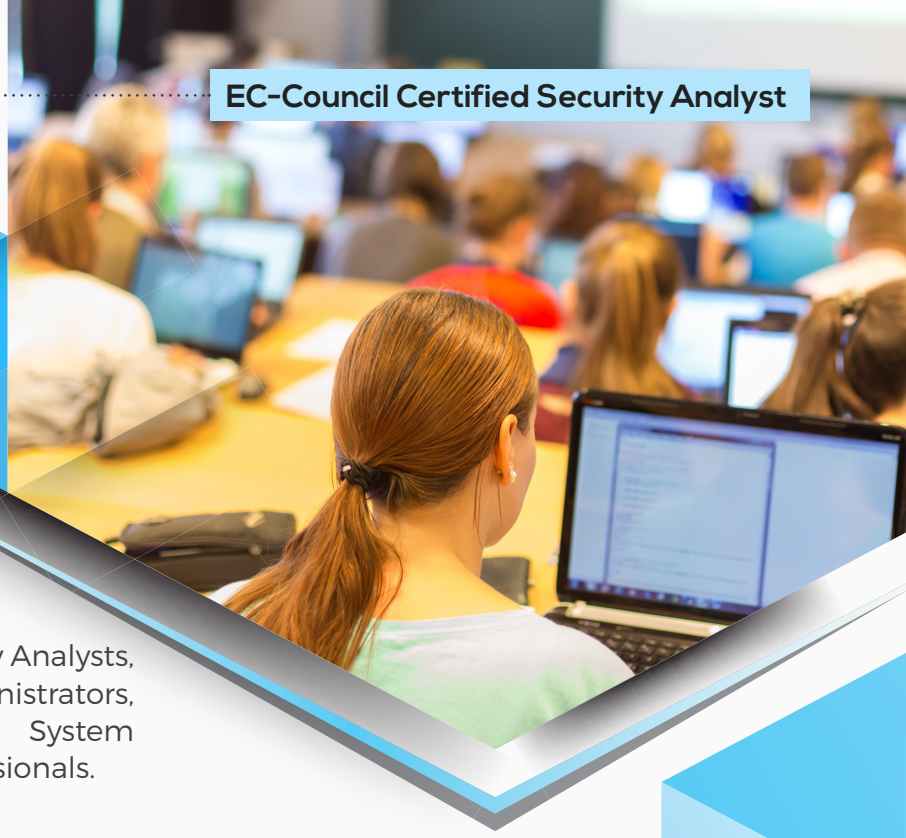
Our web portal enables you to launch an entire range of target machines and access them remotely with one simple click. It is the most cost effective and easy to use live range lab solution available.

With iLabs, lab exercises can be accessed 24x7, allowing the student to practice skills in a safe and fully functional network anytime it is convenient.

Our guided step-by-step labs include exercises with detailed tasks, supporting tools, and additional materials as well as our state-of-the-art "Open Environment" allowing you to launch a complete live range open for any form of hacking or testing.

Available target machines are completely virtualized, allowing you to control and reset machines





Who Should Attend

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

Suggested Duration

5 days (9:00am - 5:00pm)
Minimum 40 hours

ECSA Exam:

The ECSA exam aims to test a candidate's knowledge and application of critical penetration testing methodologies.

Candidates that successfully pass the multiple-choice exam will be awarded the ECSA credential.

As a powerful addition to the ECSA exam, the new ECSA (Practical) exam is now available adding even more value to the ECSA certification.

Eligibility Criteria for ECSA Exam

- Attend offical training via an EC-Council accedited training channel
  Or
- Possess a minimum of 2 years of working experience in a related InfoSec domain

> *With more than 10 years of experience in security, I never finish learning and the CCISO course reinforces all my knowledge, gives me an update and new ideas to be practical not only in my business but also in my daily life. Thanks EC-Council.*
>
> ***- Fernando Ramírez Orozco,***
> *SID Security Manager, Cable & Wirelees*

Outline of ECSA v10

1. Introduction to Penetration Testing and Methodologies
2. Penetration Testing Scoping and Engagement Methodology
3. Open Source Intelligence (OSINT) Methodology
4. Social Engineering Penetration Testing Methodology
5. Network Penetration Testing Methodology - External
6. Network Penetration Testing Methodology - Internal
7. Network Penetration Testing Methodology - Perimeter Devices
8. Web Application Penetration Testing Methodology
9. Database Penetration Testing Methodology
10. Wireless Penetration Testing Methodology
11. Cloud Penetration Testing Methodology
12. Report Writing and Post Testing Actions

EC-Council is one of the potential certification for any security professional. The study materials are highly informative and up-to-date. I recommend this certificate to all security professionals who love to learn cutting edge technology in security and are passionate about hacking.

- Imran Liaquat,
Assistant Manager Cyber Security, EY Ford Rhodes

Self Study Modules

Professional penetration testers are required to continue learning throughout their career, keeping closely engaged to the fast changing cybersecurity industry. To enable continuous learning, the ECSA course comes packed with tons to self-study resources.

1. Penetration Testing Essential Concepts

This is an Essential Prerequisite as it helps you to prepares you the ECSA courseware. Serves as a base to build Advanced Pen Testing Concepts

2. Password Cracking Penetration Testing
3. Denial-of-Service Penetration Testing
4. Stolen Laptop, PDAs and Cell Phones Penetration Testing
5. Source Code Penetration Testing 6. Physical Security Penetration Testing
6. Surveillance Camera Penetration Testing
7. VoIP Penetration Testing
8. VPN Penetration Testing
9. Virtual Machine Penetration Testing
10. War Dialing
11. Virus and Trojan Detection
12. Log Management Penetration Testing
13. File Integrity Checking
14. Telecommunication and Broadband Communication Penetration Testing
15. Email Security Penetration Testing
16. Security Patches Penetration Testing
17. Data Leakage Penetration Testing
18. SAP Penetration Testing
19. Standards and Compliance
20. Information System Security Principles
21. Information System Incident Handling and Response
22. Information System Auditing and Certification

Attaining The Industry's Most Comprehensive Methodology Based Pen Testing Certification

ECSA v10

Exam Title:
EC-Council Certified Security Analyst v10

Number of Questions: 150

Duration: 4 hours

Availability: ECC Exam Centre

Test Format: Multiple Choice

Passing Criteria: 70%

ECSA (Practical)

Exam Title:
EC-Council Certified Security Analyst (Practical)

Number of challenges: 8

Duration: 12 hours

Availability: Aspen- iLabs

Test Format: iLabs cyber range

Passing Score: 5 out of 8 challenges and submission of an acceptable penetration testing report

ECSA (Practical)

ECSA (Practical) is a 12 hours' rigorous practical exam. ECSA (Practical) presents you with a simulated organization and its underlying networks, each containing multiple hosts.

The candidates are required to demonstrate the application of penetration testing methodology presented in the ECSA program to perform a comprehensive security audit of the organization. You will start with challenges requiring you to perform advanced network scans beyond perimeter defenses, leading to automated and manual vulnerability analysis, exploit selection, customization, launch and post exploitation maneuvers.

ECSA (Practical) also tests your skills to perform threat and exploit research, skills to understand exploits in the wild, writing your own exploits, customize payloads and your ability to make critical decisions at different phases of a pen testing engagement that can make or break the whole assessment. You will also be required to create a professional pen testing report with essential elements and guidance for the organization in the scenario to act on.

The ECSA (Practical) credential provides an assurance that the candidate possesses the skills required on the field and will stand a testimony of your ability to undergo the rigor of the profession.

About the Exam:

12 hours rigorous, online proctored practical exam

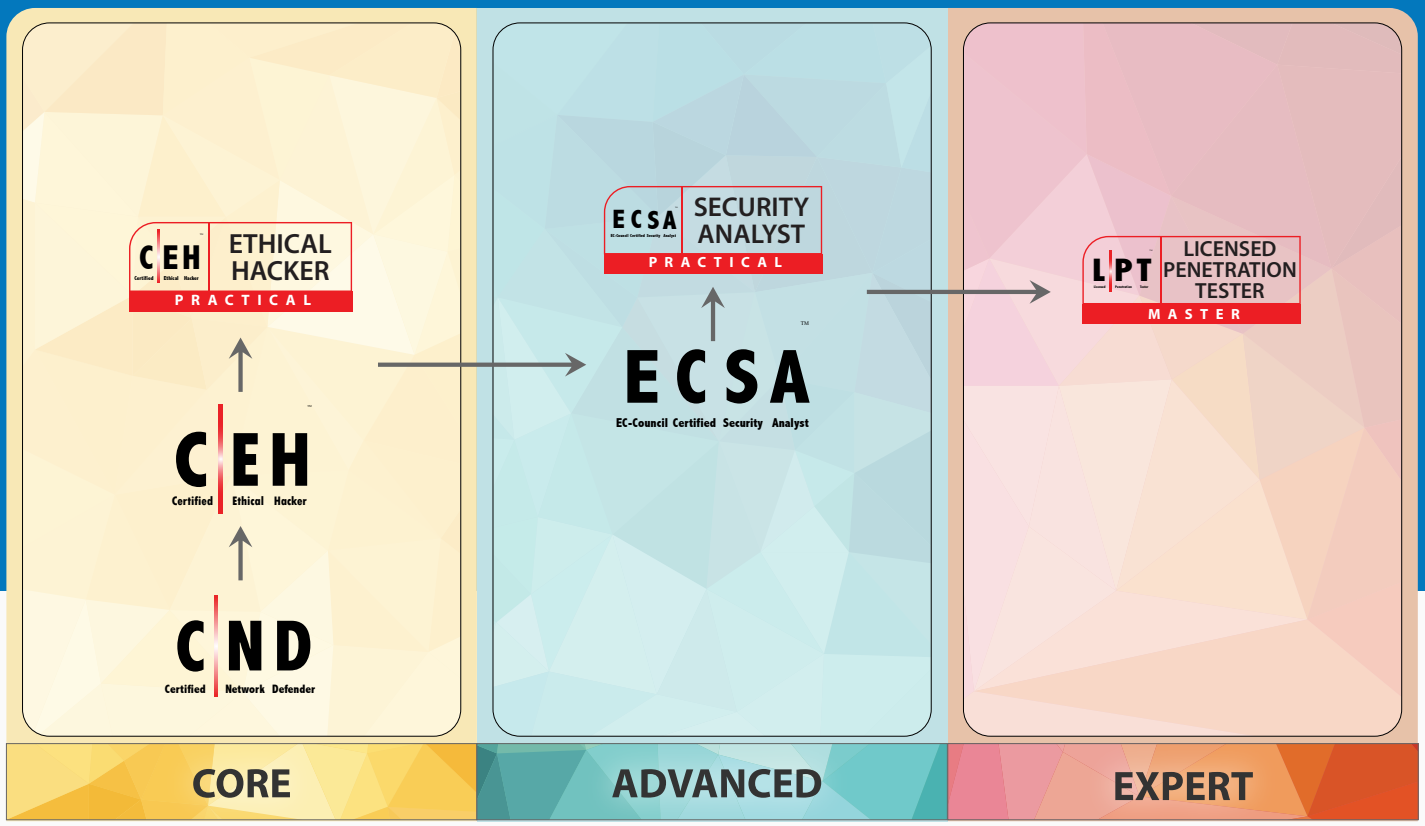
Eligibility Criteria for ECSA (Practical) Exam

To be eligible to apply to sit for the ECSA (Practical) Exam, candidate must either:

- Be an ECSA member in good standing (Your USD 100 application fee will be waived);
- or Have a minimum of 2 years working experience in InfoSec domain (You will need to pay USD 100 as a non-refundable application fee);
- or Have any other industry equivalent certifications such as OSCP or GPEN cert (You will need to pay USD 100 as a non-refundable application fee).

EC-Council VAPT Track

EC-Council's cybersecurity programs and credentials are organized into tracks to allow professionals to specialize in a particular domain or gain advancements with added recognition and skills, one after the other.



CND is the world's most advanced network defense course that covers 14 of the most current network security domains any individuals will ever want to know when they are planning to protect, detect, and respond to the network attacks. The course contains hands-on labs, based on major network security tools and to provide network administrators real world expertise on current network security technologies and operations.

CEH is the world's most advanced ethical hacking course covering 20 of the most important security domains any individual will need when they are planning to beef-up the information security posture of their organization. The course provides hacking techniques and tools used by hackers and information security professionals.

To provide employers with the confidence that you not only know your stuff, but can do the job, challenge the CEH (Practical) exam to proof your skills.

ECSA is a globally respected penetration testing program that covers the testing of modern infrastructures, operating systems, and application environments while teaching the students how to document and prepare professional penetration testing report. This program takes the tools and techniques covered in CEH to next level by utilizing EC-Council's published penetration testing methodology.

Employers can today trust not only know your knowledge in pentesting, but your skills when you produce your ECSA (Practical) credential to proof your skills.

The Advanced Penetration Testing program is the capstone to EC-Council's entire information security track, right from the CEH to the ECSA Program. The course brings advanced pentesting skills not covered in the ECSA course offering students even more advanced techniques employed by experienced pentesters.

The LPT (Master) exam covers the entire Penetration Testing process and lifecycle with keen focus on report writing, required to be a true professional Penetration Tester.

Each program offers domain specific knowledge, training and ability to prepare a professionals through their job requirements bringing career advancement and opportunities.

Click on this link to find out more details about each certification and complete the VAPT track to attain industrys' most sought after credentials.

> *I sat for the ECSA V9 exam on December of 2016 and was awarded the title of EC-Council Certified Security Analyst. What an honor. I must say that the presentation of the training and the hands-on portion of every EC-Council program that I have taken has made the difference. I have to admit that the 30-day ECSA prerequisite of submitting a pentesting report was the most challenging yet rewarding experience of my certification journey. EC-Council has hit it out of the park with this certification and the prerequisite. It forces the candidate to prove through hands on that they can implement the knowledge gained from the class rather than just being a good test taker.*
>
> ***- Cameron G. Mitchell, MS, ECSA, CHFI, CEH, ITILV3 ,***
> *CEO,*
> *Double Helix Cyber Security Solutions*

EC-Council

www.eccouncil.org