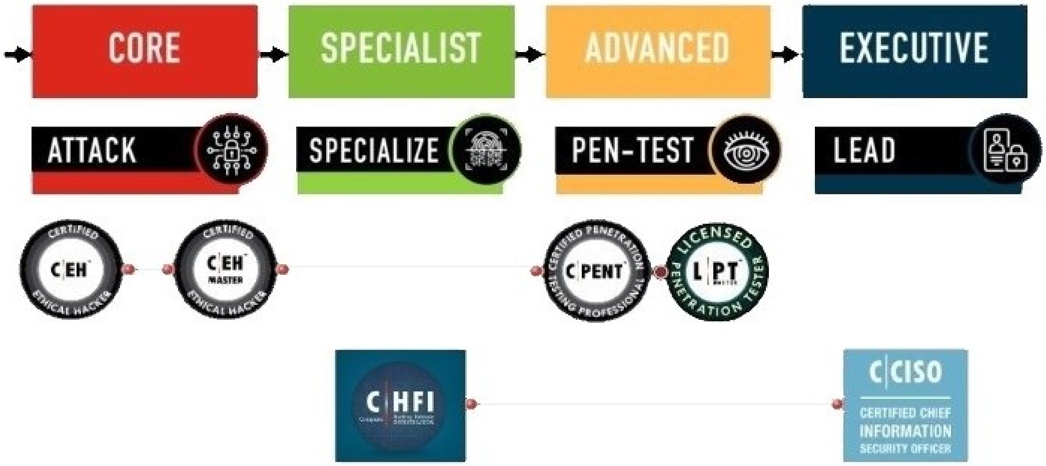
EC-Council
Hackers are here. Where are you?

SCORPIONSHIELD


CORE
SPECIALIST
ADVANCED
EXECUTIVE
ATTACK
SPECIALIZE
PEN-TEST
LEAD
C|EH CERTIFIED ETHICAL HACKER
C|EH MASTER CERTIFIED ETHICAL HACKER
C|PENT CERTIFIED PENETRATION TESTING PROFESSIONAL
L|PT MASTER LICENSED PENETRATION TESTER
C|HFI
C|CISO CERTIFIED CHIEF INFORMATION SECURITY OFFICER

SCORPIONSHIELD
ACADEMY

EC-Council Accredited Training Center

TRAINING EC-Council PARTNER

EC-Council C|EH CERTIFIED

EC-Council C|EH MASTER CERTIFIED

EC-Council C|PENT CERTIFIED

EC-Council L|PT LICENSED PENETRATION TESTER MASTER CERTIFIED

EC-Council C|HFI CERTIFIED

EC-Council C|CISO CERTIFIED

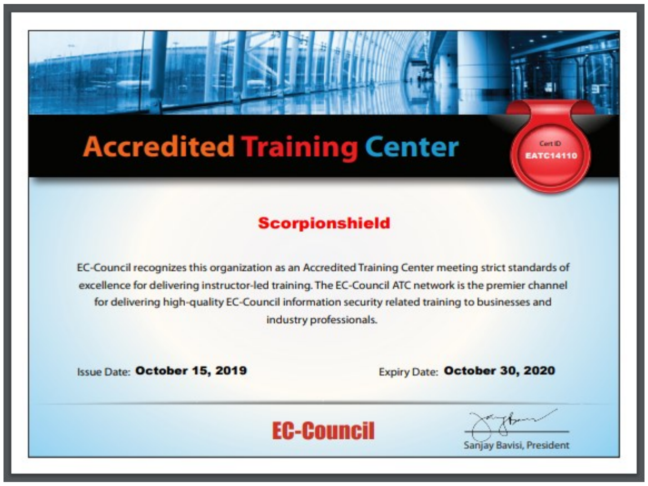
INFORMATION SECURITY & CYBERSECURITY ACADEMY
FULL EC-COUNCIL CERTIFICATION BOARD (C|CISO + C|EH + C|EH MASTER + C|HFI)

ABOUT EC-COUNCIL AND SCORPIONSHIELD

With years of experience, EC-COUNCIL is today the most reputed Cybersecurity training Organization in the World. It has the capabilities and expertise to take your cybersecurity training to the next level.

At SCORPIONSHIELD, we combine EC-COUNCIL insights and skills to transform your processes and strategies, but also your security staff training, and in turn, your company. We're proud to help shape and improve how our client's structure and manage their information security. SCORPIONSHIELD has a close partnership with EC-COUNCIL, to provide a local academy in information security, for all to be constantly upgraded in the necessary skills needed, to excel on projects.

We are an EC-COUNCIL Accredited Training Center, and our trainers are certified instructors from EC-COUNCIL.



Accredited Training Center

Cert ID
EATC14110

Scorpionshield

EC-Council recognizes this organization as an Accredited Training Center meeting strict standards of excellence for delivering instructor-led training. The EC-Council ATC network is the premier channel for delivering high-quality EC-Council information security related training to businesses and industry professionals.

Issue Date: **October 15, 2019** Expiry Date: **October 30, 2020**

EC-Council

Sanjay Bavisi, President

TIMELINE

The SCORPIONSHIELD Academy Program comprises 6 months in part-time, 4 weeks per month, 2 sessions per week, post-working hours, from 19h30 to 22h30, 3 hours per session. Hence, equivalents to 144 hours, which represents 40 hours per specific type of training to grants along with the 3 vouchers included, for attaining the 3 certifications - CEH, CHFI and CCISO. Albeit, there are extra 24 hours for the CEH Practical, which enables the additional desired certificate of CEH MASTER.

EC-COUNCIL PENTESTER PATH

To attain a level of EXPERT, from CORE and through ADVANCED, EC-COUNCIL sets the standards through 5 levels of training and certification. Scorpionshield follow this Track through a specific Academy, with the objective of develop guided Licensed Penetration Testers.

EC-Council
C|EH Certified Ethical Hacker
CERTIFIED
EC-Council
C|EH Certified Ethical Hacker MASTER
CERTIFIED
EC-Council
C|PENT Certified Penetration Testing Professional
CERTIFIED
EC-Council
L|PT LICENSED PENETRATION TESTER MASTER
CERTIFIED

EC-Council
THE NEXT BIG THING
IN CYBERSECURITY SKILL DEVELOPMENT IS HERE
CERTIFIED C|ND NETWORK DEFENDER
CERTIFIED C|EH ETHICAL HACKER
CERTIFIED PENETRATION C|PENT TESTING PROFESSIONAL
LICENSED PENETRATION L|PT TESTER MASTER

Course	Training	Exam
C|EH CERTIFIED ETHICAL HACKER V11	40 h	4 h
C|EH MASTER (PRACTICAL)	24 h	6 h
CPENT CERTIFIED PENETRATION TESTER PROFESSIONAL	24 h	12 h
L|PT LICENSED PENETRATION TESTER MASTER (PRACTICAL)	24 h	18 h

EC-Council C|EH - Certified Ethical Hacker v11

DESCRIPTION

The world’s most advanced ethical hacking course with 20 of the most current security domains an ethical hacker will want to know when planning to beef up the information security posture of their organization. In 20 comprehensive modules, the course covers over 340 attack technologies, commonly used by hackers.

Our security experts have designed over 204 labs which mimic real time scenarios in the course to help you “live” through an attack as if it were real and provide you with access to over 3500 commonly used hacking tools to immerse you into the hacker world.

The goal of this course is to help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation.

TARGET AUDIENCE

Ethical hackers, System and Network Administrators, Engineers, Web-managers, Auditors, Security Professionals.

DURATION

40 hours

EXAM

Exam Title: Certified Ethical Hacker V11 (ANSI)
Number of Questions: 125
Duration: 4 hours
Test Format: Multiple Choice
Exam Prefix: 312-50

OUTLINE C|EH

Module 01: Introduction to Ethical Hacking
Module 02: Footprinting and Reconnaissance
Module 03: Scanning Networks
Module 04: Enumeration
Module 05: Vulnerability Analysis
Module 06: System Hacking
Module 07: Malware Threats
Module 08: Sniffing
Module 09: Social Engineering
Module 10: Denial-of-Service
Module 11: Session Hijacking
Module 12: Evading IDS, Firewalls, and Honeypots
Module 13: Hacking Web Servers
Module 14: Hacking Web Applications
Module 15: SQL Injection
Module 16: Hacking Wireless Networks
Module 17: Hacking Mobile Platforms
Module 18: IoT Hacking
Module 19: Cloud Computing
Module 20: Cryptography

EC-Council Certified Ethical Hacker Practical (CEH MASTER)

DESCRIPTION

To be placed at the tip of your organization’s cyber spear, you must be confident, proficient in your job, and be at the top of your game. You must be able to think on your feet, act quickly, appropriately, and proportionally. Make a mistake and bad things can happen. CEH Master gives you the opportunity to prove to your employer, your peers, and most importantly to yourself that you can in fact take on and overcome challenges found in everyday life as an Ethical Hacker. To prove this, though, we don’t give you exam simulations.

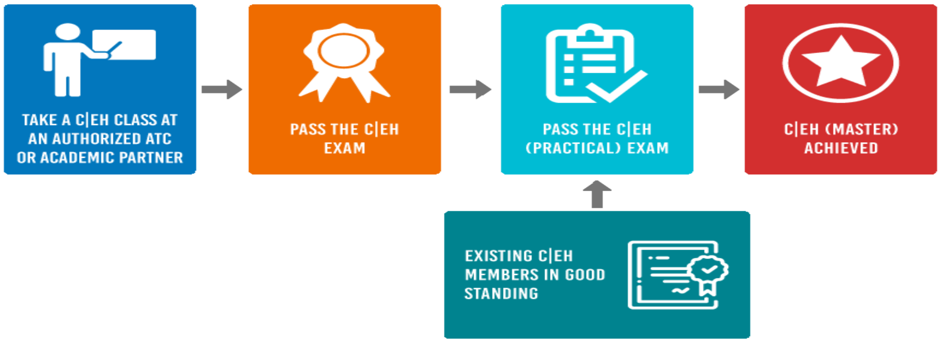
We test your abilities with real-world challenges in a real-world environment, and with a time limit, just as you would find in your job. Do you run towards danger? Do you take charge during unsettling and challenging times? Do you want to be the one your team can rely on to take the fight to the bad guys? If your answers are yes, prove yourself with CEH Master!

WHAT IS C|EH MASTER

CEH Master is the brainchild of our CEO, Jay Bavisi. It is the next evolution for the world-renowned Certified Ethical Hacker program, and a logical ‘next step’ for those holding this prestigious certification. CEH is meant to be the foundation for anyone seeking to be an Ethical Hacker. The CEH Practical Exam was developed to give Ethical Hackers the chance to prove their Ethical Hacking skills and abilities.

Earning the CEH Master designation is your way of saying, “I learned it, I know it, I proved it.” To earn the CEH Master designation you must successfully demonstrate your knowledge of Ethical Hacking through two distinctly different proving grounds.

First, you must attempt and successfully pass the ANSI Accredited Certified Ethical Hacker (CEH) multiple choice exam. Once you complete this first step, you can move on to the second part of earning the CEH Master designation, the CEH Practical Exam.


TAKE A C|EH CLASS AT AN AUTHORIZED ATC OR ACADEMIC PARTNER
PASS THE C|EH EXAM
PASS THE C|EH (PRACTICAL) EXAM
C|EH (MASTER) ACHIEVED
EXISTING C|EH MEMBERS IN GOOD STANDING

TARGET AUDIENCE AND PRE-REQUISITES

It’s the hands-on Exam of CEH Practical Certification, so pre-requisite is 312-50 CEHv11 passing score.

DURATION

24 hours

EXAM

Exam Title: Certified Ethical Hacker (Practical)
Number of Practical Challenges: 20
Duration: 6 hours
Availability: Aspen – iLabs
Test Format: iLabs Cyber Range
Passing Score: 70%

MASTER OF ETHICAL HACKING
C|EH Certified Ethical Hacker
C|EH Certified Ethical Hacker MASTER
C|EH ETHICAL HACKER PRACTICAL

EC-Council Certified Penetration Tester Professional (CPENT)

DESCRIPTION

The heart of the CPENT program is all about helping you master your pen testing skills by putting them to use on our live cyber ranges. The CPENT ranges were designed to be dynamic in order to give you a real-world training program, so just as targets and technology continue to change in live networks, both the CPENT practice and exam ranges will mimic this reality as our team of engineers continue to add targets and defenses throughout the CPENT course's lifetime.

WHAT IS ECSA

EC-Council's Certified Penetration Tester (CPENT) program teaches you how to perform an effective penetration test in an enterprise network environment that must be attacked, exploited, evaded, and defended. If you have only been working in flat networks, CPENT's live practice range will teach you to take your skills to the next level by teaching you how to pen test IoT systems, OT systems, how to write your own exploits, build your own tools, conduct advanced binaries exploitation, double pivot to access hidden networks, and also customize scripts/exploits to get into the innermost segments of the network.

The CPENT Challenge Edition is a low-cost study resource that will provide a refresher in areas such as IoT, ICS, SCADA, and binary analysis. The CPENT Challenge Edition includes a selection of labs from each of the CPENT course modules that will introduce you to the concepts that are required to obtain the required points across the different zones.

The CPENT range consists of entire network segments that replicate an enterprise network — this is not a computer game simulation; this is an accurate representation of an enterprise network that will present the latest challenges to the pen tester. The benefit of hands on learning in a live cyber range is that candidates will encounter multiple layers of network segmentation, and the CPENT course will teach candidates how to navigate these layers, so that once access is gained in one segment, a candidate will know the latest pivoting techniques required to reach the next. However, that won't be enough on its own as the targets and segments are progressive in nature, so once you get into one machine and or segment, the next one will challenge you even more.

CPENT is a fully online, remotely proctored practical exam that challenges candidates through a grueling 24-hour performance-based, hands-on exam. The exam is broken into 2 practical exams of 12-hours each that will test your perseverance and focus by forcing you to outdo yourself with each new challenge. Candidates have the option to choose either 2 12-hour exams or one 24-hour exam. Candidates who score more than 70% will earn the CPENT certification. Candidates who score more than 90% attain the prestigious LPT (Master) credential.

TARGET AUDIENCE AND PRE-REQUISITES

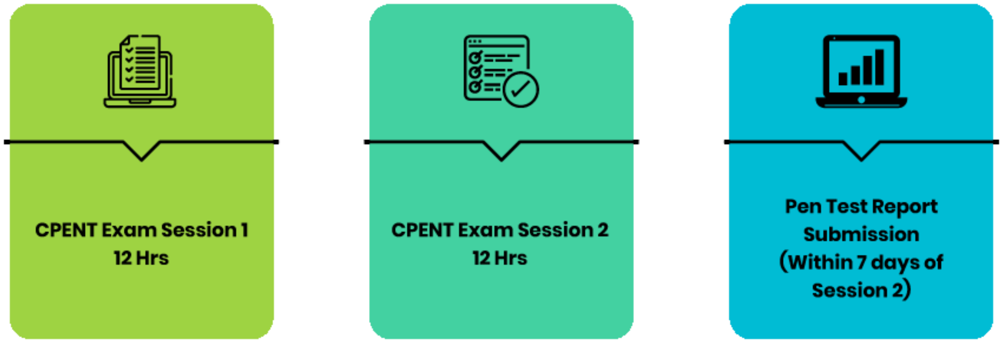
Ethical Hackers; Penetration Testers; Network server administrators; Firewall Administrators; Security Testers; System Administrators; Risk Assessment professionals;

DURATION

40 hours

You have the potential to earn two certifications with one exam. If you score above a 90% on the CPENT live range exam, not only will you earn the CPENT certification, but you will also earn the Licensed Penetration Tester (LPT) Master Credential. To be a LPT (Master) means that you can find chinks in the armor of defense-in-depth network security models with the help of network pivoting, making exploit codes work in your favor, or by writing Bash, Python, Perl, and Ruby scripts. The live range CPENT exam demands that you think on your feet, be creative in your approach, and not rely on the conventional techniques.

Outsmarting and out maneuvering the adversary is what sets you apart from the crowd. The CPENT's hands-on exam offers a challenge like no other by simulating a complex network in real time. This experience will test your perseverance and focus by forcing you to outdo yourself with each new challenge.



CPENT Exam Session 1
12 Hrs

CPENT Exam Session 2
12 Hrs

Pen Test Report Submission (Within 7 days of Session 2)

EXAM

Exam Title: CPENT Exam:

- **Credit Towards Certification:** CPENT
- **Practical:** iLABS
- **Passing Score:** 70% (90% for LPT degree)
- **Test Duration:** 12 Hours or 24 Hours

Exam features:

- Choose your challenge! Either two 12-Hour sessions or a single 24-Hour exam!
- EC-Council specialists proctor the entire exam – Validity is not in question.
- Score at least 70% and become a CPENT
- Score at least 90% and earn the highly regarded LPT (Master) designation!

OUTLINE

Module 01: Introduction to Penetration Testing
Module 02: Penetration Testing Scoping and Engagement
Module 03: Open Source Intelligence (OSINT)
Module 04: Social Engineering Penetration Testing
Module 05: Network Penetration Testing – External
Module 06: Network Penetration Testing– Internal
Module 07: Network Penetration Testing – Perimeter Devices
Module 08: Web Application Penetration Testing
Module 09: Wireless Penetration Testing
Module 10: IoT Penetration Testing
Module 11: OT/SCADA Penetration Testing
Module 12: Cloud Penetration Testing
Module 13: Binary Analysis and Exploitation

EC-Council
LPT LICENSED PENETRATION TESTER MASTER
CERTIFIED
L | P T
Licensed Penetration Tester
LICENSED PENETRATION TESTER
MASTER

EC-Council Licensed Penetration Tester Practical (LPT MASTER)

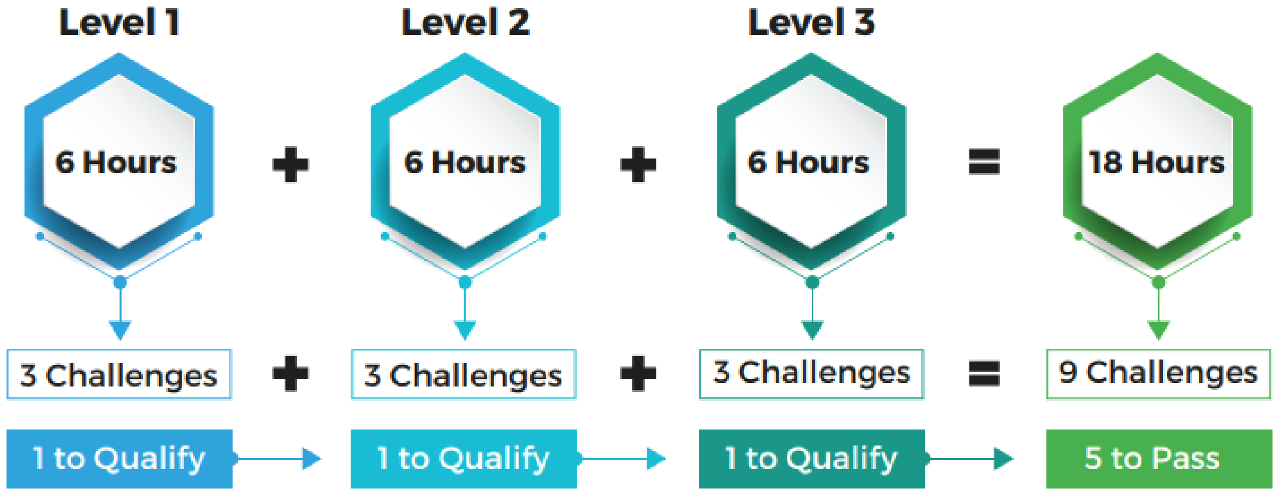
DESCRIPTION

This exam has one purpose: To Differentiate The Experts From The Novices In Penetration Testing!

There are good penetration testers and then there are great penetration testers.

Unless you are bent on being nothing other than the best in penetration testing, don’t bother registering for this program, as you are probably not cut out for it. We know that the only way to find out what you are made of is by testing you at the brink of exhaustion — which is why the LPT (Master) exam is 18 hours long!

Your pen testing skills will be challenged over three levels, each with three challenges, against a multi-layered network architecture with defense-in-depth controls. You will be required to make knowledgeable decisions under immense pressure at critical stages while selecting your approach and exploits.


Level 1 | Level 2 | Level 3

6 Hours + 6 Hours + 6 Hours = 18 Hours

3 Challenges + 3 Challenges + 3 Challenges = 9 Challenges

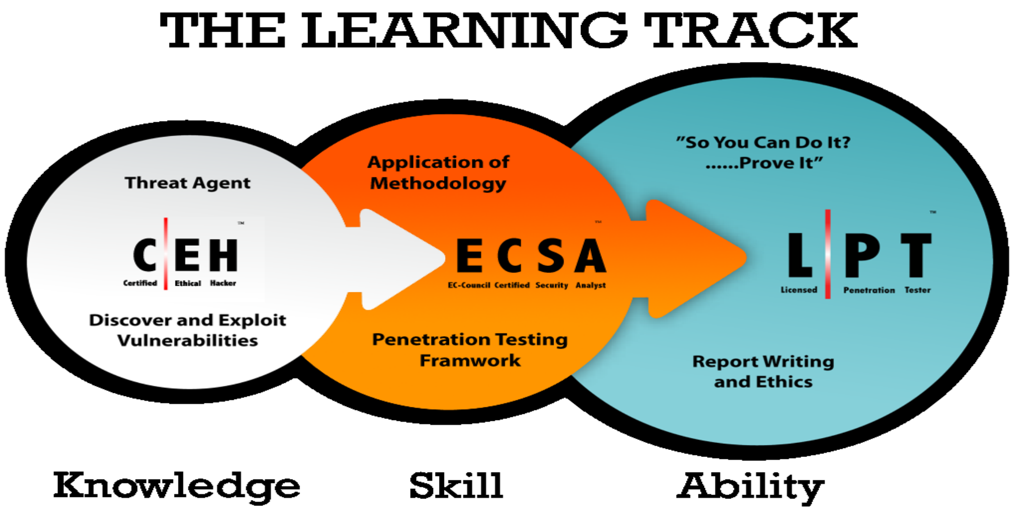
1 to Qualify → 1 to Qualify → 1 to Qualify → 5 to Pass

As you progress along these levels, you will need to maneuver web application, network, and host penetration testing tools and tricks in an internal and external context to ultimately pwn the hosts and exfiltrate data required for the completion of the challenges.

The exam will require you to demonstrate mastery of deploying advanced pen testing techniques and tools including multi-level pivoting, OS vulnerabilities exploits, SSH tunnelling, host-based application exploits, privilege escalation, web server and web application exploitation such as arbitrary local and remote file upload, SQL injection and parameter manipulation, etc – all in a real life scenario on hardened machines, networks, and applications.

WHAT IS EC-Council Licensed Penetration Tester Practical (LPT MASTER)

To introducing the World's Most Advanced Penetration Testing Program, You must understand the Learning Track behind EC-COUNCIL. First C|EH teaches to discover and exploit vulnerabilities, then ECSA the penetration testing techniques and framework, and last L|PT to learn how to be the best penetration tester.


THE LEARNING TRACK
Threat Agent
C|EH
Certified Ethical Hacker
Discover and Exploit Vulnerabilities
Application of Methodology
ECSA
EC-Council Certified Security Analyst
Penetration Testing Framwork
"So You Can Do It? ......Prove It"
L|PT
Licensed Penetration Tester
Report Writing and Ethics
Knowledge
Skill
Ability

The Advanced Penetration Testing Course by EC-Council was created as the progression after the ECSA (Practical) to prepare those that want to challenge the Licensed Penetration Tester (Master) certification and be recognized as elite penetration testing professionals. Our training has been designed by the best in the industry and meant to push you to develop the kind of skill that you've been waiting to acquire.

LPT (Master) training is not comfortable (and the exam is even worse!) but filled with intense stress meant to illicit the best from you. Those who prevail will have developed an instinctual and intellectual response to real world penetration testing challenges. Our aim is to push you to your limit while making you solve complex problems that actual penetration testers solve daily in the real world. For four punishing and long days, you will have to perform various tasks until it becomes second nature.

This program is radically different from the ECSA. In the ECSA course, you are provided guidance on what machines to attack and an initial starting point. In the Advanced Penetration Testing Course, you are presented with minimal network information along with a Scope of Work (SOW). The course was created to provide you with advanced concepts that will help when it comes to attempting the LPT (Master) Certification exam.

Demonstrate the Mastery of Advanced Pen Testing Concepts and Techniques Including:

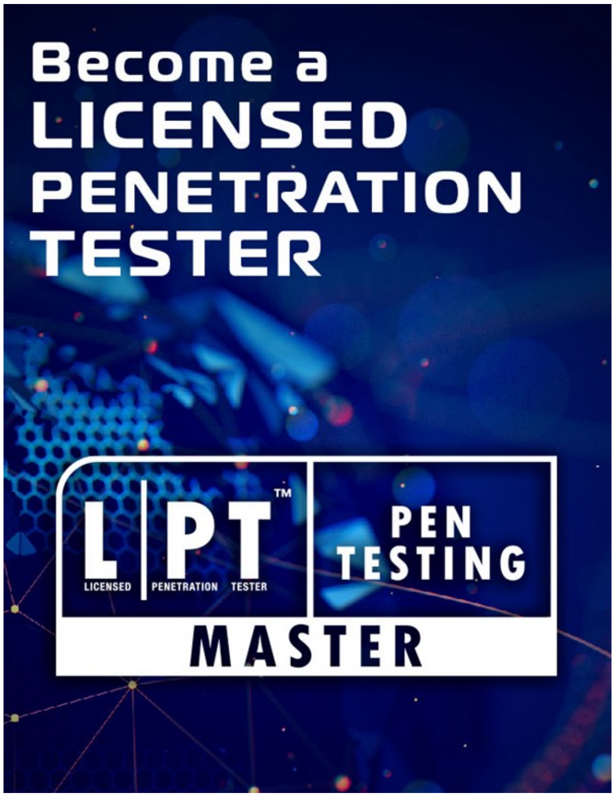
- Multi-level Pivoting
- OS Vulnerabilities Exploitation
- SQL Injection
- Host-Based Application Exploitation
- Privilege Escalation
- RFI/LFI
- Exploit and Payload Customization
- SSH Tunnelling

In this course you will learn professional security and penetration testing skills. The course is designed to show advanced concepts like scanning against defenses, pivoting between networks, deploying proxy chains, and using web shells. The last module of the course includes a SOW for each of the various networks we have created for the course. This, combined with the composition of v

arious ranges, mimics a professional penetration test. Time is limited and you will be required to identify the attack surface followed by the weaknesses of the machines that are on the network.

In summary, only those who possess the burning desire to succeed will make it.

WHAT IS EC-Council Advanced Penetration Testing Cyber Range (ECCAPT)



The Advanced Penetration Testing course from EC-Council is built on the backbone of the Advanced Penetration Testing Cyber Range (ECCAPT) and this was designed by experts who each have more than 25 years of professional security testing across the globe.

The program comes with multiple ranges designed to hone a specific set of real-life pen testing skills. The ECCAPT contains more than 180 machines with more than 250 GB RAM and more than 4000 GB of storage segregated in complex network ranges with multiple militarized and demilitarized zones. It facilitates learning and demonstration of current attack vectors, penetration testing methodology, and tools. A typical range consists of 5 to 8 subnets where each subnet represents a different business unit and comprises semi-hardened and hardened machines with more than 15 Windows and Linux OS flavors.

The range is designed to provide challenges across every level of the attack spectrum. Additionally, the range contains multiple layers of network segmentation, and once access is gained in one segment, the latest pivoting techniques are required to reach the next segment.

Many of the challenges will require outside-the-box thinking and customization of scripts and exploits to get into the innermost segments of the network. The key to be a highly skilled penetration tester is to go up against a variety of targets that are configured in a variety of ways. The ECCAPT consists of entire network segments that replicate an enterprise network — this is not a computer game simulation; this is an accurate representation of an enterprise network that will present the latest challenges to the pen tester. Since the targets and technology continue to change, the ECCAPT is dynamic and machines and defenses will be added as they are observed in the wild. Finally, the targets and segments are progressive in nature, once you get into one machine and or segment, the next one will challenge you even more.

The final range consists of challenges that will require the skills and concepts that have been covered in the course and consist of multiple visible as well as hidden subnets to prepare you for the possible challenges of the LPT (Master) range.

Finally, the ranges are designed to teach professional-level skills to identify the attack surface of targets within a required time frame and, once this has been accomplished, to gain access to the machines and escalate privileges as required. The greater the variety of targets you encounter with and without defenses, the better of a professional penetration tester you will become.

The practical environment ranges progress in difficulty and reflect real enterprise network architecture. This environment includes defenses and challenges which you must defeat and overcome.

This is not your typical flat network! As you progress through the range levels, each encounter will present the top defenses of today and you will learn the best and latest evasion techniques.

This training format has helped thousands of penetration testers globally and is proven to be effective. The ECCAPT is 100% hands-on. Everything presented in the course is through an enterprise network environment that must be attacked, exploited, evaded, and defended.

TARGET AUDIENCE AND PRE-REQUISITES

To be eligible to apply to attempt the LPT (Master) Exam, candidate must either:

- be an ECSA member in good standing;
- or, Attend the Advanced Penetration Testing course.
- or, possess a minimum of 2 years of Penetration Testing work experience in Penetration Testing;
- or, possess any other industry equivalent certifications such as OSCP or GPEN cert.

LPT (Master) certified professionals can:

- Demonstrate a repeatable and measurable approach to Penetration Testing
- Perform advanced techniques and attacks to identify SQL injection, Cross site scripting (XSS),
- LFI, RFI vulnerabilities in web applications
- Perform privilege escalation to gain root access to a system Demonstrate 'Out-of-the-box'
- and 'lateral' thinking
- Get access to proprietary EC-Council Penetration Testing methodologies
- Exploit vulnerabilities in Operating systems such as Windows, Linux
- Identify and bypass perimeter protections: In an enterprise network their will be protections, you will learn how to identify the protections in place and bypass them to extract the data even when protected with IPS and endpoint protections
- Perl, Python and Ruby scripting for the penetration tester: As a practitioner you have to be able to modify and change the methods of attacking an enterprise network, this requires custom scripting to defeat signature and anomaly-based protection mechanisms
- Advanced post exploitation and persistence: Gaining access is a small part of a professional penetration test, once you have the access, the ability to move laterally, and exfiltrate the data from the enterprise requires post exploitation skills
- Extending Metasploit with custom modules and exploits: To use open source code in a penetration test requires knowledge of the modules, and the ability to customize them based on the data you have obtained from the targets
- Pivoting from external into internal networks: Virtually all enterprise networks have external facing machines as well as internal intranet machines, the preferred way to access these is through pivoting and using the initial source of access to leverage your way into the enterprise intranet
- Avoiding the most common mistakes when drafting a professional penetration testing report: Having skills is one thing, but being able to provide tangible findings to the enterprise client is critical for a professional penetration tester

DURATION

24 hours

EXAM

Exam Title: LPT (Practical) Exam:

- Number of challenges: 9
- Duration: 18 hours
- Availability: ECCAPT
- Test Format: iLabs ECCAPT cyber range
- Passing Score: 5 out of 9 challenges
- Submission: penetration testing report

OUTLINE

Module 1. Introduction to Vulnerability Assessment and
Module 2. Penetration Testing
Module 3. Information Gathering Methodology
Module 4. Scanning and Enumeration
Module 5. Identify Vulnerabilities
Module 6. Exploitation
Module 7. Post Exploitation
Module 8. Advanced Tips and Techniques
Module 9. Preparing a Report

EC-Council Computer Hacking Forensics Investigator (CHFI) v9.0

This course will provide participants necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute in the court of law.

Every crime leaves a trail of evidence
Become a Digital Forensic Investigator
Scanning
CHFI
Computer Hacking Forensic INVESTIGATOR

COURSE OBJECTIVES

Computer forensics enables the systematic and careful identification of evidence in computer related crime and abuse cases. This may range from tracing the tracks of a hacker through a client's systems, to tracing the originator of defamatory emails, to recovering signs of fraud.

TARGET AUDIENCE

Police and other laws enforcement personnel, Defense and Military personnel, e-Business Security professionals, Systems administrators, Legal professionals, Banking, Insurance and other professionals, Government agencies, involved in the field of defense and security, familiar with the virtual world and online security issues, professionals from the world of banking and insurance, professionals with some experience in law and legal aid, government officials and IT persons with experience in dealing with cybercrimes.

PRE-REQUISITES

The work of a computer hacking forensic investigator asks for highly skilled professionals with an excellent and intimate knowledge of cyber security. Candidates must also possess excellent auditing and reporting skills. They must possess the know-how to immediately detect a security breach and take steps to recover. A great deal of patience is required in order to sift through the mountain of information on the web to find evidence of a cybercrime.

DURATION

40 hours

EXAM

Exam Title: Certified Computer Hacking Forensics Investigator (ANSI)
Number of Questions: 150
Duration: 4 hours
Test Format: Multiple Choice
Exam Prefix: 312-49

OUTLINE

1 - COMPUTER FORENSICS AND INVESTIGATIONS AS A PROFESSION
2 - UNDERSTANDING COMPUTER INVESTIGATIONS
3 - WORKING WITH WINDOWS AND DOS SYSTEMS
4 - MACINTOSH AND LINUX BOOT PROCESSES AND DISK STRUCTURES
5 - THE INVESTIGATORS OFFICE AND LABORATORY
6 - CURRENT COMPUTER FORENSICS TOOLS
7 - DIGITAL EVIDENCE CONTROLS
8 - PROCESSING CRIME AND INCIDENT SCENES
9 - DATA ACQUISITION
10 - COMPUTER FORENSIC ANALYSIS
11 - E-MAIL INVESTIGATIONS
12 - RECOVERING IMAGE FILES
13 - WRITING INVESTIGATION REPORTS
14 - BECOMING AN EXPERT WITNESS
15 - COMPUTER SECURITY INCIDENT RESPONSE TEAM
16 - LOGFILE ANALYSIS
17 - RECOVERING DELETED FILES
18 - APPLICATION PASSWORD CRACKERS
19 - INVESTIGATING E-MAIL CRIMES
20 - INVESTIGATING WEB ATTACKS
21 - INVESTIGATING NETWORK TRAFFIC
22 - INVESTIGATING ROUTER ATTACKS
23 - THE COMPUTER FORENSICS PROCESS
24 - DATA DUPLICATION
25 - WINDOWS FORENSICS
26 - LINUX FORENSICS
27 - INVESTIGATING PDA
28 - ENFORCEMENT LAW AND PROSECUTION
29 - INVESTIGATING TRADEMARK AND COPYRIGHT INFRINGEMENT

EC-Council Certified Chief Information Security Officer v3

DESCRIPTION

EC-Council's CCISO Program has certified leading information security professionals around the world. The CCISO Advisory Board contributed by forming the foundation of the program and outlining the content that would be covered by the exam, body of knowledge and training. Some members of the Board contributed as authors, others as exam writers, others as quality assurance checks and still others as trainers. Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program. The Certified CISO (CCISO) program is the first of its kind training and certification program aimed at producing top-level information security executives.

The CCISO does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view. The program was developed by sitting CISOs for current and aspiring CISOs. In order to sit for the CCISO exam and earn the certification, candidates must meet the basic CCISO requirements. Candidates who do not yet meet the CCISO requirements but are interested in information security management can pursue EC-COUNCIL Information Security Management (EISM) certification

C|CISO
Certified Chief Information Security Officer
Join the Next Generation of Information Security Leaders

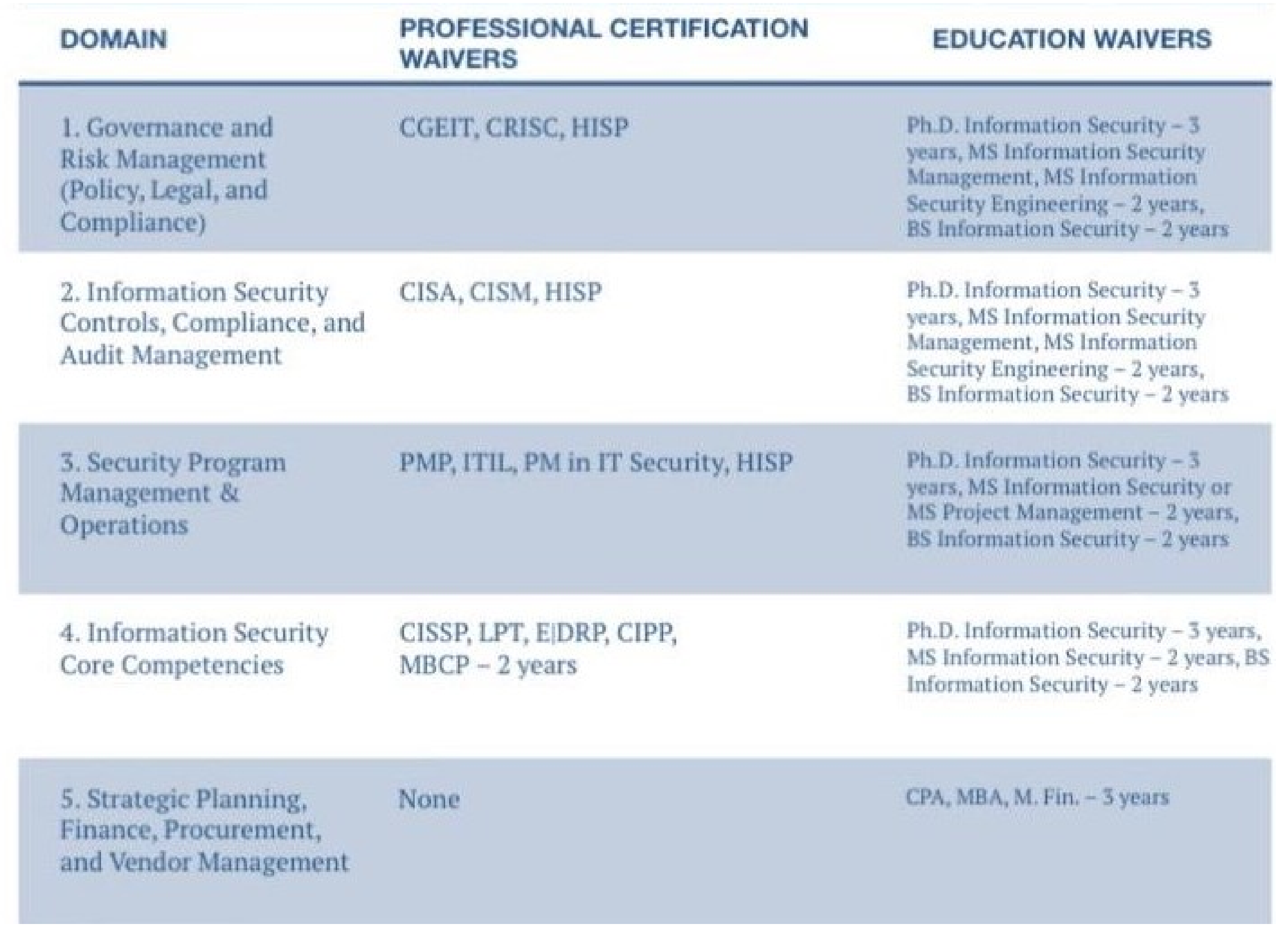
TOPICS

- Governance
- Is Risk, Controls & Auditing Management
- Information Security Leadership – Projects & Operations
- ISCoreCompetencies
- Strategic Planning & Finance

TARGET AUDIENCE AND PRE-REQUISITES

5 years' experience on 3 out of 5 Domains, or equivalent Cert Waivers / Post Grads (MS / PhD)

WAIVERS PER DOMAIN



DOMAIN	PROFESSIONAL CERTIFICATION WAIVERS	EDUCATION WAIVERS
1. Governance and Risk Management (Policy, Legal, and Compliance)	CGEIT, CRISC, HISP	Ph.D. Information Security – 3 years, MS Information Security Management, MS Information Security Engineering – 2 years, BS Information Security – 2 years
2. Information Security Controls, Compliance, and Audit Management	CISA, CISM, HISP	Ph.D. Information Security – 3 years, MS Information Security Management, MS Information Security Engineering – 2 years, BS Information Security – 2 years
3. Security Program Management & Operations	PMP, ITIL, PM in IT Security, HISP	Ph.D. Information Security – 3 years, MS Information Security or MS Project Management – 2 years, BS Information Security – 2 years
4. Information Security Core Competencies	CISSP, LPT, E|DRP, CIPP, MBCP – 2 years	Ph.D. Information Security – 3 years, MS Information Security – 2 years, BS Information Security – 2 years
5. Strategic Planning, Finance, Procurement, and Vendor Management	None	CPA, MBA, M. Fin. – 3 years

DURATION

40 hours

EXAM

Exam Title: Certified Chief Information Security Officer (ANSI)
Number of Questions: 150
Duration: 2,5 hours
Test Format: Multiple Choice
Exam Prefix: 712-50

OUTLINE

Module 1. Governance
Information program security management
Information security governance program
Regulatory and legal compliance
Risk management
Module 2. Is Risk, Controls & Auditing Management
Design, Deploy and Manage Security Controls
Security Control Types and Objectives
Implement Control Assurance Frameworks Audit Management
Module 3. Information Security Leadership – Projects & Operations
The role of the CISO
Information security projects
Integration of security into processes (change management, version control, disaster recovery, etc.)
Module 4. Information Security Core Competencies
Access controls
Physical security
Disaster recovery and business continuity planning
Network security
Threat and vulnerability management
Application security
Encryption
Vulnerability assessments and penetration testing
Computer forensics and incident response
Module 5. Strategic Planning & Finance
Security Strategic Planning and Alignment with Business Goals and Risk Tolerance
Key Performance Indicators (KPI)
Financial Planning
Development of business cases for security
Analyzing, forecasting, and developing a capital expense budget and an operating expense budget
Return on investment (ROI) and cost-benefit analysis
Vendor management and integrating security into contractual agreement and procurement process