As cybercriminals’ increasingly sophisticated tactics continue to disrupt businesses and organizations globally, coordinated and concerted defense strategies have become indispensable. To strengthen cybersecurity infrastructures today, we need constructive and collaborative efforts from all stakeholders. At EC-Council, we are committed to equipping security professionals with the cutting-edge knowledge and skills necessary to safeguard digital ecosystems. Our initiatives reflect our goal to create a strong and skilled cybersecurity workforce.

Jay Bavisi,
President & CEO, EC-Council Group
The recent surge in cyberattacks targeting countries’ critical infrastructures has heralded a new phase of cyberwarfare. Attacks on public services can have devastating consequences, disrupting both individuals’ daily lives and business operations. Iran’s state television recently announced that authorities had foiled cyberattacks that intended to target more than 100 public sector agencies. We are now at a critical juncture in cybersecurity, with threat actors ready to exploit any vulnerabilities or oversights in security practices.

Countries have gradually become more conscious of the importance of cybersecurity, given the risks of leaving data and networks unprotected. In light of the ongoing conflict in Europe and the constant expansion of attack surfaces, businesses and government agencies alike must amp up their defenses and implement holistic cyber hygiene practices. In last month’s Locked Shields event—a live-fire cyber defense exercise organized by NATO—the cyber range included a simulation of a central bank’s reserve management and financial messaging systems for the first time in its 12-year history.

The increasing and tangible costs of cyberattacks make it essential for cybersecurity professionals to arm themselves with information to keep hackers at bay. In addition, organizations must create robust security cultures by ensuring that their employees receive cybersecurity training. The April 2022 issue of EC-Council’s Cyber Brief offers critical insights from security experts, engaging webinars with industry leaders, success stories from alumni of our certification programs, and updates on the latest trends and challenges in cybersecurity. We hope you find these resources informative and valuable.

Access EC-Council Cyber Brief Previous Issues »

Success Stories

How the C|EH Elevated My Career
- Diane Bramos

How the C|EH Helped Fill the Gaps in My Cybersecurity Education
- Cyrus Mousavi
Penetration Testers

How the C|EH Helped Me Build a Strong Career in Cybersecurity
- Ryan R. May

How the C|EH Helped Me Progress in My Career
- Kevin Keller

Brazil Tops March 2022 Global Ethical Hacking Leaderboard

How C|PENT Strengthened My Real-World Pen Testing Skills
- Amit Agarwal

Ethical Hacking Leaderboard

Success Stories
How Can Penetration Testing Prevent Social Engineering Attacks?

Exploring Next-Generation Penetration Testing Techniques in the C|PENT Course

Insights

Penetration Testing Phases

Reconnaissance
Reconnaissance requires the tester to collect as much information on the testing subject as possible, including personnel, technology, and systems information.

01 Pre-engagement
In the pre-engagement penetration testing phase, the tester and client define the scope of the penetration test, such as what systems will be tested, what methods the tester will use, and any additional goals and legal implications.

02 Exploitation
All identified vulnerabilities are exploited at this stage in accordance with the scope outlined in the pre-engagement phase.

03 Threat Modeling
After collecting sufficient information on the client's system, testers then begin modeling realistic threats that the client will face before scanning for the relevant vulnerabilities in the system that those attacks would normally target.

04 Reporting
The tester generates a penetration testing report for the client that describes the methods that were used, what vulnerabilities were exploited, what remedial actions should be undertaken, and any other relevant information.

05 Post-exploitation
Once the testing time has run out or all relevant systems have been exploited, all testing methods and vulnerabilities—including associated devices, ports, or personnel—are recorded.

06 Re-testing
After the client has had time to resolve the vulnerability issues outlined in the initial report, the tester can return to run the same penetration tests on the client’s system to verify that the vulnerabilities have been resolved. This phase is not as common but may be requested by the client.

07 How C|PENT Took My Penetration Testing Skills to the Next Level
- Harith Dilshan
Threat Intelligence Analysts

Six Best Practices for Secure Network Firewall Configuration

Network Defenders

Insights

Becoming an Incident Handler: Why Getting Certified Matters

Incident Handlers

Insights

What Are the Responsibilities of a Security Operations Center Team?

Security Operations Center Analysts

Insights

The C|CT: A Brand-New Cybersecurity Course to Kickstart Your Professional Career

Cybersecurity Technicians

Insights

Launch Your Cybersecurity Career with EC-Council's C|CT Certification
Chief Information Security Officers

The Top 10 Qualities of a Successful CISO

Why Conducting Cyber Risk Assessments Is Critical for 21st-Century Businesses

Chief Information Security Officers

Why a Successful CISO Pursued the C|CISO - Richard Foltak

How the C|CISO Program Helped Miguel Ribeiro Transform His Career

Cloud Security Engineers

Master Cloud Security Skills with EC-Council’s C|CSE Program
In a world where cyberattacks make headlines every day, cybersecurity professionals and career starters need a wide range of skills to stay on top of their responsibilities and keep up with the evolving industry. Rise above the rest and progress in your cybersecurity career with CodeRed's Ultimate Cybersecurity Career Builder Bundle, available for a limited time at 40% off—just $29.99! Interested in improving your skills in a specific field of cybersecurity? Buy any of the 15 courses in the bundle for just $3.99 each.

EC-Council in the Media

World Leader in Cybersecurity Education Partners with Renowned College to Address New Zealand’s Cybersecurity Talent Gap
Webinars

Webinar Recordings

How SOCs Can Evolve in an Era of Advanced Cyberattacks

Zero-Day Vulnerability Response: A Case Study of Log4j

Why Addressing Cybersecurity Vulnerabilities Is a Top Priority

Skills, Trends, and Challenges in Modern Network Defense
Webinars

What Is the Future of Cybersecurity?

Ethical Hacking: Emerging Technologies That Require Red Teamers

Upcoming Webinars

- Threat Intelligence: Moving Towards Cyber Resilience in 2022
  - Register

- Going Green with Proof-of-Stake Blockchain Protocols
  - Register

- Cyberthreat Hunting and Intelligence in Internet of Things (IoT) Environments
  - Register
How to Bridge the Skills Gap in the Cybersecurity Industry

Understanding the Responsibilities of a Chief Information Security Officer

Read, Share, and Stay Updated!

Brought to You by EC-Council