As businesses embrace modern technologies for scalability in today's digitization era, the risks of new threats and vulnerabilities cannot be overlooked. Cybercriminals have caused damage to both corporate and government organizations in recent years, underlining the importance of investing in cybersecurity initiatives and promoting cyber awareness. EC-Council is committed to bolstering cybersecurity awareness and equipping security professionals with the most up-to-date resources and skills. Everyone must work together to strengthen cybersecurity infrastructure, and our monthly newsletter is simply one step in that direction.

- Jay Bavisi, President and CEO of EC-Council Group
Cybersecurity has become a global concern, as evidenced by the recent surge of cybercrimes. Ransomware attacks, exploiting vulnerabilities, social engineering techniques, and nation-state affiliated cybercrimes all pose a significant threat to cybersecurity. Geopolitical tensions are also a major driver for cyberwarfare among nations, and there is no doubt that organized crimes are gaining momentum as well. As cybercriminals leverage sophisticated technologies and techniques to exploit vulnerabilities and launch malware campaigns, there is a greater need to stay informed—staying upskilled and cyber aware falls on all of us. The May 2022 Cyber Brief from EC-Council offers insights from seasoned cybersecurity professionals, thought-provoking webinars from industry leaders, inspiring success stories from our successful alumni on their certification journeys, and the latest industry updates and resources. We hope you find these resources informative and valuable.

Penetration Testers

C|PENT Labs Prepare Penetration Testers for Real-Life Scenarios
- Rasmus Christensen

C|PENT Review, Preparation Tips, and Cyber Range Experience: Advice From a Licensed Penetration Tester (Master)
Common Penetration Testing Mistakes

01. Failing to Plan
Planning is essential for any penetration test. Without a plan, the tester will miss important targets and waste time gathering irrelevant data.

02. Not Knowing Your Tools
Knowing which tools to use and how to use them is essential for any penetration tester. Using the wrong tool for the job can lead to wasted time and false positives.

03. Testing Too Early
Testing too early in the process can lead to inaccurate results. The tester needs to understand the environment and the vulnerabilities that exist to perform a good test.

04. Relying on Automation
Automated tools can be a great time saver, but they should never be relied on exclusively. Automated tools can miss things that human testers would easily find, so it's essential to always manually review the results of an automated scan.

Incident Handlers

TIPS FOR CLOUD INFORMATION SECURITY

1. Avoid storing sensitive information in the cloud when possible
2. Encrypt data or use cloud services that offer local encryption
3. Restrict access by deploying multifactor authentication
4. Use strong and unique passwords
5. Install antivirus software
6. Create a backup with a different cloud provider or on an external storage device
7. Regularly monitor your organization’s cloud environment
8. Avoid using public Wi-Fi networks
THE TOP SIX TYPES OF WEB APP SECURITY VIOLATIONS IN 2021

1. Predictable Resource Location
2. SQL and Code Injection
3. Cross-site Scripting (XSS)
4. Path Traversal
5. Server Information Leakage
6. Security and Server Misconfigurations

THE THREE LEVELS OF THREAT INTELLIGENCE

Operational Threat Intelligence
- Relates to the nature, intent, and capabilities of specific threats and attacks
- Often provided in a combination of human- and machine-readable formats and handled by network defenders

Tactical Threat Intelligence
- Covers the network’s strengths, vulnerabilities, and defenses
- Used to understand how a malicious actor would attack an organization

Strategic Threat Intelligence
- Paints a general picture of the effects and possibilities of a cyberattack
- Used by stakeholders and board members to make organizational strategy decisions
What Is Incident Management and What Are Its Advantages?

Understanding Digital Forensics In Under 5 Minutes

EC-Council

Ethical Hackers

EC-Council

Ethical hacking is used to counter cyberattacks by anticipating the methods hackers might use to infiltrate a network. Ethical hackers identify potential system vulnerabilities so organizations can rectify them before they can be exploited.

The C|EH v11 course covers basic to advanced hacking concepts, including deep dives into the five phases of hacking.
2 SCANNING
This phase is an extension of active reconnaissance. The hacker extracts information through scanning devices, such as dialers, port scanners, network mappers, ping tools, and vulnerability scanners.

3 GAINING ACCESS
In this phase, the actual hacking takes place. Hackers use the vulnerabilities identified in the reconnaissance and scanning phases to access the targeted system, network, and associated applications.

4 MAINTAINING ACCESS
In this stage, the hacker attempts to gain system ownership. Hackers employ tools like keyloggers, backdoors, etc., to access the system for further exploitation and attacks.

5 COVERING TRACKS
In this final phase, the hackers attempt to hide their activity. They cover their tracks by deleting activity logs, uninstalling applications, closing open ports, and tampering with system logs. These actions erase evidence of hacking activity, making it difficult to trace where they originated.

C|EH Leaderboard

India Tops April 2022
Global Ethical Hacking Leaderboard
C|EH Practical
How to prevent CSRF attacks?

There are three fundamental approaches that you can apply to your application’s CSRF mitigation strategy to prevent CSRF attacks and eliminate vulnerabilities:

1. Using CSRF tokens in HTML forms for critical operation requests in applications
2. Avoiding using the HTTP GET method for critical operations, such as create, update, and delete actions
3. Using the "SameSite" attribute of the HTTP "Set-Cookie" response header
How Pen Testing and Hacking Skills Can Boost Your Cloud Security Career

Upskilling is necessary at every stage to stay relevant and to continue learning in the cybersecurity industry. Professionals who don’t upskill are more likely to face professional stagnation, experience lower job satisfaction, and earn less pay than their peers. Upgrade your cybersecurity skills desired by employers with CodeRed’s Buy-One-Get-One-Free offer on the 15-course bundle. This offer is also applicable for individual courses. Hurry up! This offer is valid for a limited time only.

Why a Successful CISO Pursued C|CISO

Richard Foltak

Explore the bundle!
Webinar Recordings

Improving Ransomware Resistance by Enhancing Network Security

Core Digital Forensics Skills for Investigating Cyber Incidents

Threat Intelligence: Moving Towards Cyber Resilience in 2022

Cyberthreat Hunting and Intelligence in Internet of Things (IoT) Environments
Upcoming Webinars

- Secure and Resilient Public Services
- The Dos and Don'ts of API Security
- Network Security Essentials: Attacks and Defense Strategies
- Does Remote Work Present a Major Cybersecurity Threat?
- How CISOs Should Approach Critical Cloud Security Issues
EC-Council in the Media

**Cybersecurity Leader Celebrates the Very Best of Ethical Hackers in Annual Report**

**EC-Council Partners with PwC to Boost Cybersecurity in the Middle East**

**Students Gain Industry Advantage Through University’s Partnership with Cybersecurity Leader**
Five Jobs You Can Get with a Bachelor's Degree in Cybersecurity

What Can You Do with a Master's Degree in Cybersecurity?

How a Master's Degree from EC-Council University Can Advance Your Cybersecurity Career