Tutelr. / NEXA360

TIAC CERTIFICATIONS
Tutelr Information Assurance Certification

Advanced Ethical Hacking Certification Program

TEHC
Ethical Hacking Certification

6 Month Program | 36 CPEs | Laptop Required

You Will Learn

- In-depth skills for testing network security.
- Mastery of advanced hacking methods.
- Identifying system vulnerabilities effectively.
- Encryption and secure data practices.
- Preventing common software vulnerabilities.
- Safeguarding applications from attacks.
- Protecting cloud setups and IoT devices.
- Efficiently managing security breaches.
- Responsible and ethical hacking practices.
- Staying updated on evolving risks.
- Real-world simulations for practical learning.
- Guidance from experienced professionals.
- Potential readiness for industry certifications.

TEHC
Ethical Hacking Certification

TIAC Ethical Hacking Certification

- Engage in live simulations as a "Red Team" member, testing your skills against real-time challenges.
- Delve into the security intricacies of interconnected IoT devices and their vulnerabilities.
- Gain a rare understanding of securing blockchain technology and smart contracts.
- Learn to dissect and understand malware through reverse engineering techniques.
- Understand and counteract advanced techniques used by hackers to evade detection.
- Explore strategies to safeguard vital infrastructure against cyber threats.

The Advanced Ethical Hacking Course offered by Tutelr is an exceptional educational program that delves deep into the intricacies of ethical hacking, equipping individuals with advanced skills and knowledge to navigate the complex world of cybersecurity. As discussed in our previous conversations, Tutelr has established itself as a reputable institution in the field of cybersecurity education, known for its comprehensive and hands-on approach. This course is designed for professionals seeking to elevate their ethical hacking abilities to an advanced level. It covers an extensive range of topics including network penetration testing, vulnerability assessment, advanced exploitation techniques, cryptography, secure coding practices, and more.

One of the key highlights of this course is its practical orientation. Participants are provided with real-world scenarios and hands-on labs that simulate actual hacking situations, enabling them to apply theoretical concepts in a controlled environment. The course also emphasizes the importance of ethical conduct, teaching participants how to responsibly identify vulnerabilities and safeguard systems against malicious attacks.

Tutelr's team of experienced instructors, as previously mentioned, comprises industry experts who bring a wealth of knowledge to the table. Their guidance ensures that students gain insights into the latest hacking trends, defensive strategies, and emerging technologies. Furthermore, the course is tailored to accommodate both beginners and experienced professionals, making it accessible to a wide range of learners.

Upon completion of the Advanced Ethical Hacking Course, participants can expect to have an in-depth understanding of advanced hacking techniques, security protocols, and mitigation strategies. This not only enhances their career prospects in the cybersecurity field but also empowers them to contribute significantly to safeguarding digital landscapes from cyber threats. Tutelr's commitment to excellence and the quality of their course, as previously discussed, makes them a top choice for individuals seeking to excel in the realm of ethical hacking.

“This course taught me to truly focus on the methodology while performing a pen test. During the Capture-the-Flag event, I realized how much time can be wasted if you fail to respect your methodology.”

-Sandya Jalesh - Security Engineer, **Shell Corp.**

www.tutelr.org/train-and-certify/courses

Discover how to take this course : Online

Module Descriptions

Module 1: Introduction to Ethical Hacking

Our Introduction to Ethical Hacking is your passport to a thrilling journey through the ethical hacking landscape. Discover the art of safeguarding systems, unravel vulnerabilities, and wield cybersecurity strategies like a pro. Unleash your inner detective as you learn to think like a hacker, with a twist of morality. Join us to master the techniques that secure the digital realm while embracing the thrill of the hack - the ethical way.

TOPICS:

- **Understanding Ethical Hacking**
- **Ethics and Legal Aspects in Hacking**
- **Types of Hackers and Hacking Methodologies**
- **Penetration Testing Frameworks**
- **Setting up a Hacking Lab Environment**

MODULE 3: Scanning and Enumeration

Dive into the heartbeat of cybersecurity as we demystify the art of scanning and enumeration. Journey through the digital landscape, uncovering hidden pathways, and revealing the secrets of network exploration.

TOPICS:

- **Network Scanning Techniques**
- **Port Scanning and Service Enumeration**
- **Vulnerability Scanning**
- **Banner Grabbing and SNMP Enumeration**
- **NetBIOS and SMB Enumeration**

MODULE 5: Web Application Hacking

Dive into the heart of the online realm as you master the art of uncovering vulnerabilities, cracking codes, and fortifying defenses. This electrifying journey takes you behind the scenes of web technology, where you'll unravel hidden weaknesses and harness your newfound prowess to bolster cybersecurity. Unleash your inner digital detective and rewrite the rules of the virtual frontier through hands-on challenges and real-world simulations.

TOPICS:

- **Web Application Security Basics**
- **Cross-Site Scripting (XSS) Attacks**
- **SQL Injection Attacks**
- **Cross-Site Request Forgery (CSRF)**
- **Web Application Vulnerability Scanners**

MODULE 7: Cryptography and Cryptanalysis

Delve into the art of crafting unbreakable codes and deciphering hidden messages. Join us on a journey where ciphers become puzzles and encryption turns into a thrilling game of strategy. From ancient techniques to cutting-edge algorithms, learn to wield the power of secrecy and uncover the mysteries that lie beneath the surface.

TOPICS:

- **Basics of Cryptography**
- **Encryption Algorithms and Protocols**
- **Cryptanalysis Techniques**
- **Steganography**
- **Cryptography Tools and Utilities**

Module 2: Footprinting and Reconnaissance

Discover the art of tracing digital footprints and master the craft of reconnaissance in the cyber realm. Dive into this captivating course to unravel hidden trails, decode online secrets, and learn how to map the virtual landscape like never before. Unleash your inner investigator and navigate the vast web of data, leaving no corner unexplored. Join us to become the ultimate online sleuth and wield the power of information to safeguard the digital domain

TOPICS:

- **Information Gathering Techniques**
- **Passive and Active Reconnaissance**
- **Google Hacking and Open Source Intelligence (OSINT)**
- **Social Engineering for Reconnaissance**
- **Tools and Techniques for Footprinting**

Module 4: System Hacking and Exploitation

Delve into the exhilarating world of cybersecurity as we peel back the layers of systems, revealing their vulnerabilities and empowering you to safeguard the digital realm. Discover the art and science behind ethical hacking, as we guide you through the maze of exploits, penetration testing, and ingenious techniques. Gain the power to expose weaknesses before malicious actors do, and master the fine balance between offense and defense. Get ready to wield knowledge that's both coveted and critical in today's digital landscape. Are you ready to breach and defend?"

TOPICS:

- **Password Cracking Techniques**
- **Privilege Escalation Methods**
- **Exploiting Vulnerabilities**
- **Metasploit Framework**
- **Post-Exploitation Activities**

MODULE 6: Wireless Network Hacking

Uncover the secrets that radio waves carry and master the art of navigating through digital airwaves. Join us on an electrifying journey where you'll learn to unravel the vulnerabilities of wireless networks, decode encryption barriers, and outsmart security protocols. From cracking the code to unlocking hidden gateways, this immersive experience will empower you to ethically explore the boundless realm of wireless connectivity. Unchain your potential with Wireless Network Hacking and redefine what's possible in the digital age

TOPICS:

- **Wireless Networks Fundamentals**
- **Wi-Fi Encryption and Attacks**
- **Rogue Access Points**
- **WPA/WPA2 Cracking**
- **Wireless Security Best Practices**

Who Should Attend

- IT Professionals: Individuals working in IT roles who seek to specialize in cyber security and enhance their skills to effectively protect digital assets and networks.
- Security Analysts: Those currently in security roles looking to advance their knowledge in specific areas such as penetration testing, incident response, or digital forensics.
- Network Administrators: Professionals responsible for managing and securing networks who want to broaden their understanding of cyber threats and mitigation techniques.
- System Administrators: Individuals handling system configuration and management, interested in securing systems against potential cyber attacks.
- Software Developers: Developers aiming to create secure applications by understanding vulnerabilities and incorporating robust security measures into their coding practices.
- Risk Managers: Those tasked with assessing and mitigating risks, including cyber risks, who wish to incorporate advanced cyber security strategies into their risk management approach.
- Cybersecurity Enthusiasts: Individuals passionate about cyber security, even without prior experience, looking to kickstart their career in the field and develop practical skills.
- Recent Graduates and Students: Graduates and students studying computer science, IT, or related fields who want to specialize in cyber security to meet the growing industry demand.
- Security Consultants: Those consulting organizations on security matters, aiming to expand their expertise and provide more comprehensive solutions.
- Professionals Switching Careers: Individuals transitioning from other fields into cyber security, attracted by its dynamism and the increasing need for skilled professionals.

NICE Framework Work Roles

1. Ethical Hacker/Penetration Tester
2. Security Analyst
3. Security Consultant
4. Incident Responder
5. Cybersecurity Researcher
6. Security Engineer
7. Cryptographer
8. Red Teamer
9. Threat Hunter
10. Security Auditor
11. Security Trainer/Educator
12. Malware Analyst
13. IoT Security Specialist
14. Cloud Security Engineer
15. Application Security Specialist