Cyber Security Syllabus

CEH

The Greens Technologys CEH v10 Certified Ethical Hacker training (earlier CEH v9) and certification course provide hands-on classroom training to help you master the same techniques that hackers use to penetrate network systems and leverage them ethically to protect your own infrastructure.
The extensive course focuses on 20 of the most popular security domains to provide a practical approach to essential security systems.

Key Learning Objectives

After completing this course you will be able to:

- Ace the CEH practical exam
- Learn to assess computer system security by using penetration testing techniques
- Scan, test and hack secure systems and applications, and gain hands-on experience with sniffing, phishing and exploitation tactics

Course Curriculum

- **Module 01:** Introduction to Ethical Hacking - Overview of information security, threats, attack vectors, ethical hacking concepts, information security controls, penetration testing concepts, and information security laws and standards are covered in this module
- **Module 02:** Footprinting and Reconnaissance - These modules cover concepts and types of footprinting, footprinting through search engines, web services, and social networking sites, footprinting tools, countermeasures, and footprinting pen testing

- **Module 03:** Scanning Networks - Learn about network scanning concepts, tools and techniques, network diagrams, and scanning pen testing
- **Module 04:** Enumeration - Enumeration concepts, types, techniques, and pen testing are covered in this module
- **Module 05:** Vulnerability Analysis - Overview of vulnerability assessment concepts, solutions, scoring systems, tools, and reports are explained in this module
- **Module 06:** System Hacking - Learn how to crack passwords, hide files, cover tracks, any many more
- **Module 07:** Malware Threats - This module gets you familiar with malware concepts, trojan concepts, malware analysis, countermeasures, malware penetration testing
- **Module 08:** Sniffing - Sniffing concepts, tools, and techniques are explained in this module
- **Module 09:** Social Engineering - Comprehend social engineering concepts, techniques, countermeasures, and pen testing
- **Module 10:** Denial-of-service - Dos/DDoS concepts, techniques, tools, case studies, and penetration testing are covered in this module
- **Module 11:** Session Hijacking - Know what is session hijacking and its types, tools, countermeasures, and session hijacking penetration testing
- **Module 12:** Evading IDS, Firewalls, and Honeypots - Learn about firewalls and honeypots and how to detect and evade them
- **Module 13:** Hacking Web Servers - This module focuses on web server concepts, attacks, methodologies, tools, countermeasures, and penetration testing
- **Module 14:** Hacking Web Applications - Web app concepts, tools, methodologies, countermeasures, and penetration testing are covered in this module

- **Module 15:** SQL Injection - Get familiar with SQL Injection concepts, types, tools, methodologies, countermeasures, and penetration testing
- **Module 16:** Hacking Wireless Networks - Wireless concepts, threats, methodologies are covered in this module
- **Module 17:** Hacking Mobile Platforms - Learn how to hack android IOS, Mobile spyware, device management, security tools, and many more in this module
- **Module 18:** IoT Hacking - This module covers IoT Hacking concepts, attacks, methodologies, tools, countermeasures, and penetration testing
- **Module 19:** Cloud Computing - Concepts, attacks, methodologies, tools, countermeasures, and penetration testing of cloud computing are covered in this module
- **Module 20:** Cryptography - This module will teach you about cryptography concepts, encryption algorithms, tools, PKI, types of encryption, cryptanalysis, and countermeasures