Introduction to Certified Ethical Hacker

A Certified Ethical Hacker is a specialist typically working in a red team environment, focused on attacking computer systems and gaining access to networks, applications, databases, and other critical data on secured systems. A CEH understands attack strategies, the use of creative attack vectors, and mimics the skills and creativity of malicious hackers. Unlike malicious hackers and actors, Certified Ethical Hackers operate with permission from the system owners and take all precautions to ensure the outcomes remain confidential. Bug bounty researchers are expert ethical hackers who use their attack skills to uncover vulnerabilities in the systems.

Course Description

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is recognized as a standard within the information security community. CEH v11 continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used by hackers and information security professionals today. The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: "To beat a hacker, you need to think like Animesh a hacker."

Instructor

Animesh Roy is an Application Security Researcher and Penetration Tester having more than 5 years of industrial experience with good knowledge in Vulnerability Assessment and Penetration Testing on various domains like Web Applications, Mobile Applications, APIs, and Networks. He delivered trainings to the Indian Army, Corporates, colleges and foreign delegations as well.

You can learn more about him here: https://linkedIn.com/in/anir0y

Agenda

Day	Contents
Day 1	Introduction to Ethical Hacking
Day 2	Footprinting and Reconnaissance
Day 3	Scanning Networks
Day 4	Enumeration
Day 5	Vulnerability Analysis
Day 6	System Hacking
Day 7	Malware Threats
Day 8	Sniffing
Day 9	Social Engineering
Day 10	Denial-of-Service
Day 11	Session Hijacking
Day 12	Evading IDS, Firewalls, and Honeypots
Day 13	Hacking Web Servers
Day 14	Hacking Web Applications
Day 15	SQL Injection
Day 16	Hacking Wireless Networks
Day 17	Hacking Mobile Platforms
Day 18	IoT and OT Hacking
Day 19	Cloud Computing
Day 20	Cryptography

For those candidates who don’t know the basics:

Day	Contents
Day 1	Introduction to Ethical Hacking(Windows)
Day 2	Introduction to Ethical Hacking(Linux)
Day 3	Introduction to Ethical Hacking (Mac OS)