



Kursus

5 dage

Nr. 87218 P

DKK 25.000

ekskl. moms

Dato

Sted

Certified Ethical Hacker [CEHv12]

Hack dine egne systemer, før andre gør det! Lær at scanne, teste og penetrere din virksomheds netværk og systemer, så du kan opdage hullerne, og lukke dem, før hackeren finder dem. I et hands-on miljø, lærer du at hacke etisk, så du opnår optimal Information Security Posture i din organisation. Du vil lære om malware, IoT og om, hvordan du både hacker og sikrer de mange nye produkter, der kan tilgå internettet. Undervisningen kan foregå på engelsk.

Vær to skridt foran din hacker, og opnå optimal sikkerhed

Certified Ethical Hacker (CEH) er den mest benyttede certificering og kvalificering inden for etisk hacking og anbefales af IT-arbejdsgivere overalt i verden. Den er den mest populære certificering inden for informationssikkerhed og udgør et af de hurtigst voksende cyberkvalificeringskrav blandt udbydere af kritisk infrastruktur og essentielle tjenester. Siden CEH blev lanceret i 2003, har det været anerkendt som en standard i informationssikkerhedssektoren.

CEH v11 introducerer løbende de nyeste og mest avancerede hackingredskaber og -teknikker, der anvendes af hackere og IT-sikkerhedsprofessionelle i dag. De fem faser af etisk hacking og CEH's oprindelige mission er stadig gyldige og relevante i dag: "For at bekæmpe en hacker skal du tænke som en hacker."

Certified Ethical Hacker (CEH) Version 12 Update:

CEH giver en dybdegående forståelse for de faser, etisk hacking består af, forskellige angrebsvektorer og forebyggende modforanstaltninger. På kurset lærer du, hvordan hackere tænker og udfører deres angreb, så du er i en bedre position, når du skal etablere din sikkerhedsinfrastruktur og forhindre fremtidige angreb. Når en organisation forstår systemers

svagheder og sårbarheder, kan den bedre styrke sine systemsikkerhedskontroller og minimere risikoen for databrud.

CEH blev udviklet for at implementere et miljø og en systematisk proces, der er praktisk anvendelig på tværs af alle domæner og metoder inden for etisk hacking. Det giver dig mulighed for at opbygge den viden og de færdigheder, der er nødvendige for at arbejde som ethical hacker. Du vil opleve en helt anderledes tilgang til, hvilke typer ansvar og foranstaltninger det kræver at etablere sikkerhed. I 12. udgave udbygger CEH fortsat med de nyeste operativsystemer og hackingværktøjer, -taktikker, -teknikker og teknologier.

Deltagerprofil

Kurset er for ethical hackers, systemadministratorer, netværksadministratorer og -ingeniører, webansvarlige, revisorer og sikkerhedsfolk generelt.

Har du kendskab til Windows, Linux, Netværk (TCP/IP), er du godt klædt på til at deltage på kurset.

Udbytte

- Lær om packet sniffing-teknikker, der afslører netværkssvagheder, og om modforanstaltninger mod sniffing
- Lær om vigtige problemer, der plager IT-sikkerhedsverdenen, etisk hacking, informationssikkerhedskontroller, love og standarder
- Lær at vurdere fodaftryk og rekognoscering med de nyeste footprinting-teknikker og -værktøjer
- Lær at udføre netværksscanningsteknikker og modforanstaltninger med scanning
- Lær at bruge enumerationsteknikker og modforanstaltninger mod enumeration
- Lær at udarbejde sårbarhedsanalyser, der identificerer sikkerhedshuller i organisationens netværk, kommunikationsinfrastruktur og slutsystemer
- Få viden om systemhackingmetodikker til at opdage system- og netværkssårbarheder herunder steganografi, steganalyse-angreb og sløring af spor
- Lær om forskellige typer malware (trojanske heste, virus, orme osv.), systemrevision rettet mod malwareangreb, malwareanalyse og modforanstaltninger

Det får du på arrangementet

- Certificering/eksamen
- Kursusbevis
- Fuld forplejning
- Materiale på engelsk
- Undervisning på engelsk

Indhold

The following topics are reviewed

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications



- [SQL Injection](#)
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

After this course you will be able to:

- Social engineering techniques and how to identify theft attacks to audit humanlevel vulnerabilities and suggest social engineering countermeasures.
- DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.
- Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.
- Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.
- Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.
- SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.
- Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools. Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.
- Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security techniques and tools.
- Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
- Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.

Anmeldelser af Certified Ethical Hacker [CEHv12]

Vores underviser er MEGET kompetent og en god formidler. Vi har alle haft en meget lærerig uge, i gode rammer, og i god stemning.

— **Morten Bjørn Dalmose** H. Skjøde Knudsen A/S

Materiale

Kursusmaterialet leveres på engelsk.

Certificering

The Certified Ethical Hacker exam 312-50 can be taken as an online Proctored exam to receive CEH certification. Exam voucher is included.

- Number of Questions: 125
- Test Duration: 4 Hours
- Test Format: Multiple Choice
- Passing Score: 70%

Online kurset "[Certified Ethical Hacker \(CEH\)](#)" kunne også være interessant for dig.

CEH CERTIFIED ETHICAL HACKER

What is CEH? ➔	Course Content ➔	Who is It For? ➔
CEH is the leading ethical hacking training and certification program in cybersecurity. Students audit a system for weaknesses and vulnerabilities using the same tools and exploits as malicious hackers, but under proper legal circumstances and in the best interest of assessing the security posture of a target system and organization. It teaches how hackers think and act maliciously so you can learn to better position your organization's security infrastructure and defend against future attacks.	Students will receive their study kit consisting of physical and digital course materials, including their iLabs code. iLabs will be used to complete classroom training sessions. Students will work with the instructor to review the tools and learn how to apply them to the iLabs Cyber Range.	• Information Security Analyst/Administrator • Information Assurance (IA) Security Officer • Information Security Manager/Specialist • Information Systems Security Engineer/Manager • Information Security Professionals/Officers • Information Security and IT Auditors • Risk/Threat/Vulnerability Analyst • System Administrators • Network Administrators and Engineers • Anyone who is concerned about the integrity of the network infrastructure
What is NEW in CEH V11? ➔	Course Mapping ➔	Exam Information
• The newly updated CEH V11 course now includes a library of the latest tools required by security practitioners and pen testers across the world. • It is mapped rigorously to important Specialty Areas under the NIST/NICE framework's Protect and Defend (PR) job role category • CEH has updated Cloud and IoT modules to incorporate CSPs, Container Technologies (e.g. Docker, Kubernetes), as well as Cloud Computing threats and a number of IoT hacking tools such as Shikra, Bus Pirate, Facedancer21 and more. • The program has new operating systems including Windows Server 2019, Windows Server 2016, and Windows 10 configured with Domain Controller, firewalls, and vulnerable web applications for practicing and improving hacking skills. • Includes the latest malware analysis tactics for ransomware, banking and financial malware, IoT botnets, OT malware analysis, Android malware and more. • More than 50% of the CEH v11 course is dedicated to practical skills in live ranges via EC-Council labs.	• CND • CEH • CEH (Practical) • CPENT • LPT (Master)	EXAM TITLE ĩ Certified Ethical Hacker # OF QUESTIONS ĩ 125 DURATION ĩ 4 Hours
https://cert.eccouncil.org/certified-ethical-hacker.html For More Information on Certification: https://cert.eccouncil.org/application-process-eligibility.html		

EC-COUNCIL

Hackers are here. Where are you?

Har du faglige spørgsmål så kontakt



Malene Kjærsgaard
+45 72202523
mch@teknologisk.dk