CEH with AI - Certified Ethical Hacker with AI

Corso di formazione Hacker Etico Certificato EC-Council - CEH v13

Corso di certificazione CEH v13 accreditato da EC-Council

40 ORE

Dai creatori di Certified Ethical Hacker (CEH) arriva la nuova ed evoluta versione 13 con funzionalità AI aggiunte. Strutturata in 20 moduli di apprendimento che coprono oltre 550 tecniche di attacco, CEH ti fornisce le conoscenze di base di cui ha bisogno un professionista della sicurezza informatica.

RISULTATI ATTESI:

Passo 1: Imparare

Sviluppa le tue competenze nei domini principali della sicurezza informatica con 20 moduli. Sperimenterai 221 laboratori pratici, 550 tecniche di attacco e oltre 4.000 strumenti di hacking e sicurezza.

Passo 2: Certificare

Sostieni un esame di 4 ore con 125 domande a risposta multipla e un esame pratico di 6 ore con 20 sfide reali per ottenere la certificazione CEH Master in CEH v13.

Passo 3: Ingaggiare

Applica tutto ciò che hai imparato in un impegno di hacking etico simulato. Questo impegno di sicurezza in quattro parti ti offre una vera esperienza di impegno di hacking etico dall'inizio alla fine contro un'organizzazione emulata.

Passo 4: Competere

Sfida i tuoi pari da tutto il mondo con l'accesso annuale a 12 sfide CTF da 4 ore ciascuna per migliorare le tue abilità e rimanere aggiornato sulle ultime tendenze.

39 CPE validi ai fini del mantenimento delle certificazioni ISACA

Sconto 5% per iscrizioni entro 30 giorni

Sconto 10% aggiuntivo per almeno 3 iscritti della stessa azienda

INFO: corsi@aiea-formazione.it - Tel: 02.8716.9246

MODULO D'ISCRIZIONE AL CORSO CEH with AI - Certified Ethical Hacker with AI

DATI FATTURAZIONE

Ragione Sociale - Cognome e nome	Partita iva/C.f.	Codice Destinatario/Pec
Via e Numero	**CAP**	**Città e (PR)**
E-mail Amministrazione	**Telefono Azienda**	**Nr. Ordine d'acquisto/RdA**

DATI PARTECIPANTI

Nome e Cognome	E-mail personale	Socio ISACA	Socio AIEA	ID ISACA

DATA E LOCATION: Verificare date e location sul sito www.aiea-formazione.it e specificare le proprie scelte di seguito

MODALITA' DI PAGAMENTO: Bonifico Bancario anticipato intestato a Profice
Coordinate Bancarie: IBAN:IT46 J030 3211 7020 1000 0806 292
Causale: Indicare cognome del partecipante e ragione sociale

PREZZO: Corso live in italiano + esame in inglese	SECONDA OPZIONE PREZZO: Corso elearning AUTONOMO + esame in inglese
☐ 3.490,00€ + IVA	☐ 1.790,00€ + IVA
☐ 3.390,00€ + IVA (Riservato Soci ISACA)	☐ 1.750,00€ + IVA (Riservato Soci ISACA)
☐ 3.290,00€ + IVA (Riservato Soci AIEA/ISACA MI)	☐ 1.750,00€ + IVA (Riservato Soci AIEA/ISACA MI)

AGEVOLAZIONI ☐ Sconto 5% per iscrizioni entro 30 giorni ☐ Sconto 10% aggiuntivo per almeno 3 iscritti

ACQUISTO MEMBERSHIP ISACA ☐ 250,00€ + IVA

REFERENTE ORGANIZZATIVO E AMMINISTRATIVO: Profice srl - P.iva 02487960201 - Codice Destinatario: M5UXCR1
Sede Legale: Via Fernelli, 28 - 46100 - Mantova (MN) - Tel: 02.8716.9246 - Fax: 02.8715.1741 - Email: direzione@profice.it
PARTNER DI AIEA (Associazione Italiana Information System Auditor) www.aiea-formazione.it - www.aiea.it

PRIVACY E DIRITTI DELL'INTERESSATO: I Suoi dati personali saranno trattati sia su supporto informatico che cartaceo e il loro conferimento è necessario per l'iscrizione al corso: la mancata fornitura dei dati non consentirà pertanto l'iscrizione. Accettando il presente regolamento, Lei autorizza il trattamento dei Suoi dati personali solo per fini organizzativi, contabili, e per aggiornarLa sulle nostre iniziative formative, nella piena tutela dei Suoi diritti e della Sua riservatezza e in conformità alle disposizioni di legge ai sensi del GDPR UE 679:2016 e del D.lgs. n. 101:18. Titolare del trattamento dei dati è Profice srls. In qualsiasi momento Lei potrà richiedere l'aggiornamento o la cancellazione dei Suoi dati personali scrivendo a direzione@profice.it.
RECESSO/DISDETTA : Il cliente, tramite fax o e-mail a corsi@aiea-formazione.it, potrà disdire dal contratto senza penali entro e non oltre il 15mo giorno precedente la data di inizio del corso: in questo caso Profice provvederà a rifondere l'intera quota versata. Oltre tale termine Profice potrà trattenere una penale di 50 Eu, o, qualora la richiesta di cancellazione pervenga negli ultimi 3 giorni dall'inizio corso, l'integrale quota di iscrizione.
ANNULLAMENTO DEL CORSO: Profice si riserva il diritto di annullare il corso per gravi impedimenti o per mancato raggiungimento del numero minimo di partecipanti, in qualsiasi momento, rifondendo quanto versato.
ASPETTI ORGANIZZATIVI: (1) L'iscrizione si intende perfezionata al momento del ricevimento, da parte della segreteria corsi, della presente scheda compilata in tutte le sue parti. Al raggiungimento del numero minimo di partecipanti verrà inviata una conferma d'iscrizione tramite fax o e-mail, al più tardi entro 10 giorni di calendario dalla data di inizio del corso. (2) Gli attestati verranno emessi in formato digitale successivamente alla partecipazione al corso ed a pagamento avvenuto.
PAGAMENTO: Il pagamento dovrà avvenire, a seguito della conferma inviata dalla segreteria corsi, a mezzo bonifico bancario (o Carta di Credito con 3% di sovrapprezzo)
FORMAZIONE FINANZIATA: è possibile avvalersi della Formazione Finanziata concordando con Profice gli adempimenti amministrativi prima del corso

Il Cliente previa lettura delle condizioni al presente contratto, in particolare delle clausole "aspetti organizzativi", "pagamento", "recesso/disdetta", "annullamento del corso",dichiara espressamente di approvarli specificatamente ai sensi e agli effetti di cui agli art. 1341 e 1342 cod. civ.

Data | Firma e Timbro

INVIARE MODULO a corsi@aiea-formazione.it o via FAX: 02.8715.1741

CORSO:	**CEH with AI - Certified Ethical Hacker with AI** **Corso di formazione Hacker Etico Certificato EC-Council - CEH v13**
DESCRIZIONE:	Dai creatori di Certified Ethical Hacker (CEH) arriva la nuova ed evoluta versione 13 con funzionalità AI aggiunte. Strutturata in 20 moduli di apprendimento che coprono oltre 550 tecniche di attacco, Il corso CEH fornisce tutte le conoscenze di base di cui ha bisogno un professionista della sicurezza informatica. Il corso CEH v13 è basato sull'intelligenza artificiale, è ed la prima certificazione di hacking etico al mondo che sfrutta la potenza dell'intelligenza artificiale. Permette di conoscere le tecniche basate sull'intelligenza artificiale per aumentare l'efficienza della difesa informatica del 40%, semplificando al contempo il proprio flusso di lavoro.. Il nuovo programma di studi è stato aggiornato e arricchito di contenuti per poter meglio padroneggiare le più recenti tecniche di attacco ed imparare le ultime tendenze nelle contromisure.
RISULTATI ATTESI:	Passo 1: Imparare Sviluppa le tue competenze nei domini principali della sicurezza informatica con 20 moduli. Sperimenterai 221 laboratori pratici, 550 tecniche di attacco e oltre 4.000 strumenti di hacking e sicurezza. Passo 2: Certificare Sostieni un esame di 4 ore con 125 domande a risposta multipla e un esame pratico di 6 ore con 20 sfide reali per ottenere la certificazione CEH Master in CEH v13. Passo 3: Ingaggiare Applica tutto ciò che hai imparato in un impegno di hacking etico simulato. Questo impegno di sicurezza in quattro parti ti offre una vera esperienza di impegno di hacking etico dall'inizio alla fine contro un'organizzazione emulata. Passo 4: Competere Sfida i tuoi pari da tutto il mondo con l'accesso annuale a 12 sfide CTF da 4 ore ciascuna per migliorare le tue abilità e rimanere aggiornato sulle ultime tendenze.
DURATA:	40 ORE
DESTINATARI:	Professionisti, che già lavorano come sistemisti o programmatori, che aspirano a diventare ethical hacker come arricchimento del proprio bagaglio di competenze e per cogliere le opportunità del mercato del lavoro che sempre più richiede questa figura.
PRE-REQUISITI:	- Conoscenza del protocollo TCP/IP; - Conoscenza di base dei sistemi operativi Windows; - Conoscenza di base dei sistemi operativi Linux.
CONTENUTI:	Il corso prevede un iter formativo fortemente interattivo nel quale verrà mostrato come effettuare scanning, testing e hacking dei propri sistemi al fine di renderli più sicuri. L'impiego di laboratori ed esercitazioni pratiche è mirato a dare una conoscenza approfondita unita all'esperienza concreta sui fondamentali sistemi di sicurezza. Il corso entra nel futuro della sicurezza informatica con una formazione che integra l'intelligenza artificiale in tutte le fasi dell`hacking etico. Una prima fase importante è dedicata a comprendere il funzionamento delle difese perimetriche e verranno mostrati e condotti degli scanning e attacchi alle proprie reti. Una seconda fase è dedicata ad apprendere le tecniche impiegate dagli intrusi per l'escalation dei privilegi e quali passi possono essere attuati per mettere in sicurezza un sistema. Approfondimenti specifici sono dedicati all'intrusion detection, alla policy creation, al social engineering, agli attacchi DDoS, ai buffer overflow e alla creazione di virus. . - Module 01: Introduction to Ethical Hacking Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures. - Module 02: Footprinting and Reconnaissance Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking Module 03: Scanning Networks Learn different network scanning techniques and countermeasures.

- Module 04: Enumeration
Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures.

- Module 05: Vulnerability Analysis
Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools are also included.

Module 06: System Hacking
Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks.

- Module 07: Malware Threats
Learn about different types of malware (Trojan, viruses,worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.

- Module 08: Sniffing
Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.

- Module 09: Social Engineering
Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

- Module 10: Denial-of-Service
Learn about different Denial of Service (DoS) and Distributed DoS(DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

- Module 11: Session Hijacking
Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

- Module 12: Evading IDS, Firewalls, and Honeypots
Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

- Module 13: Hacking Web Servers
Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Module 14: Hacking Web Applications
Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures.

Module 15: SQL Injection
Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.

- Module 16: Hacking Wireless Networks
Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.

- Module 17: Hacking Mobile Platforms
Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

- Module 18: IoT Hacking
Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.

- Module 19: Cloud Computing
Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools.

- Module 20: Cryptography
Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

CERTIFICAZIONE:

	CEH v13 riconosciuto da EC-Council
MATERIALE DI STUDIO:	Il costo del corso comprende tutto il materiale necessario alla formazione, oltre che l'accesso ON-LINE della durata di 6 mesi agli iLabs EC Council e agli altri strumenti online ufficiali di supporto alla formazione e alla preparazione dell'esame.
DATE E LOCATION:	Verificare Date e Location sul sito www.aiea-formazione.it prima di iscriversi
CREDITI FORMATIVI:	39 CPE validi ai fini del mantenimento delle certificazioni ISACA
NOTE:	Il corso in elearning self-paced è fornito direttamente da Profice, in qualità di EcCouncil iLearn Official Partner Il corso in presenza di docente è invece erogato da Dgroove, Partner ufficiale EC Council per i corsi dal vivo
ESAME:	Il corso prepara a sostenere l'esame EC-Council Certified Ethical Hacker v13 accreditato ANSI. Il costo del corso include il voucher d'esame Pearson Vue.
FORMAZIONE FINANZIATA:	PROFICE è certificata EN ISO 9001:2015 per il sistema di gestione per la Qualita, settori IAF/EA 35 e 37 - Certificato No. IT18-27105A del 9 Ottobre 2018 (Progettazione ed erogazione corsi di formazione professionale; Consulenza direzionale, organizzativa e di Compliance)

Chi è AIEA (ISACA Milan Chapter)

L'Associazione Italiana Information Systems Auditors - AIEA -, costituita in Milano nel 1979, riunisce coloro che in Italia svolgono professionalmente attività di Auditing e Controllo di sistemi ICT promuovendo la conoscenza e ampliando l'esperienza dei suoi aderenti nel campo dell'Information Systems Audit , Assurance, Governance e Security. L'Associazione,Capitolo di Milano di ISACA, favorisce lo scambio di metodologie, promuove un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo sia di affidabilità dell'organizzazione che di sicurezza dei sistemi. Promuove inoltre ricerche quale quella sulla Governance IT commissionata a SDA Bocconi, organizza un Convegno annuale, cura la traduzione in italiano di Val IT, COBIT®, e da oltre 15 anni del Manuale CISA e delle correlata documentazione, sostiene la diffusione delle certificazioni professionali CISA (Certified Information Systems Auditor), CISM(Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT) e CRISC (Certified in Risk and Information Systems).

Chi è ISACA

Con oltre 100.000 associati in 180 Paesi, ISACA® (www.isaca.org) è leader mondiale nel fornire competenze, certificazioni, community, patrocinio e formazione nei settori dell'assurance e sicurezza, del governo dell'impresa,della gestione dell'IT e dei rischi e della compliance correlati all'IT. Fondata nel 1969, ISACA, associazione indipendente senza fini di lucro, organizza conferenze internazionali, pubblica l'ISACA Control Journal®, e sviluppa standard internazionali relativi all'audit e al controllo dei sistemi IT, che contribuiscono a garantire i propri componenti sull'affidabilità e a trarre valore dai sistemi informativi. ISACA favorisce inoltre l'acquisizione delle competenze e delle conoscenze IT e le attesta mediante le certificazioni riconosciute a livello internazionale quali: CISA® (Certified Information Systems Auditor™),CISM® (Certified Information Security Manager®), CGEIT™ (Certified in the Governance of Enterprise ITTM) e CRISC™ (Certified in Risk and Information Systems Control™). ISACA aggiorna continuamente COBIT® che assiste i professionisti dell'IT e i manager delle imprese ad adempiere le proprie responsabilità relativamente all'IT governance e alla gestione manageriale, in particolare nell'ambito dell'assurance, sicurezza, rischio e controllo e a fornire valore al business.

Quali vantaggi per i soci AIEA

E' possibile iscriversi ad AIEA tramite ISACA, selezionando il Milan chapter (http://www.isaca.org/Membership/Join-ISACA).

I soci possono accedere a:

1) accesso gratuito
- a più di 20 Sessioni di Studio annuali, con crediti CPE utili al mantenimento delle certificazioni;
- all'ISACA eLibrary (raccolta di quasi tutte le pubblicazioni ISACA/ITGI);
- alle versioni elettroniche dei framework ISACA;
- ai webcasts e agli e-Simposi organizzati da ISACA;

2) sconti
- sulle pubblicazioni nel Bookstore ISACA;
- sulle quote d'iscrizione e sulle pubblicazioni di preparazione agli esami CISA, CISM, CGEIT e CRISC;
- su corsi ed eventi organizzati da AIEA Formazone o da altri Enti ed Associazioni in partnership o patrocinati;
- invio gratuito del magazine bimestrale ISACA Journal e delle newsletter AIEA.

Partner dei corsi AIEA Formazione