

Ethical Hacking: Come Proteggere i Sistemi dalle Minacce informatiche - FORMAZIONE A DISTANZA

INIZIO CORSO: giovedì 7 novembre 2024

DURATA: 10 ore

ORARIO LEZIONI: dalle ore 14.00 alle ore 17.30

PREZZO: 805,20 € (660,00 € + IVA)



Panoramica corso:

In questo corso intensivo, ti immergerai completamente nell'Ethical Hacking, acquisendo una solida conoscenza teorica e pratica delle tecniche utilizzate dagli hacker per penetrare i sistemi informatici.

Cosa imparerai?

- I concetti base dell'Ethical Hacking: scoprirai i principi fondamentali dell'hacking etico, le diverse tipologie di hacker e il loro modus operandi.
- Le principali metodologie di attacco informatico: apprendrai le tecniche utilizzate dagli hacker per attaccare i sistemi informatici, tra cui scansioni di vulnerabilità, ingegneria sociale, phishing, malware e attacchi DDoS.
- Strumenti e tecniche di Vulnerability Assessment: padroneggerai i migliori strumenti e le tecniche utilizzate dai Penetration Tester per identificare e sfruttare le vulnerabilità dei sistemi informatici.
- Le fasi del Penetration Test: imparerai a pianificare, eseguire e documentare un Penetration Test completo, dall'engagement iniziale al reporting finale.
- Come difendersi dagli attacchi informatici: svilupperai le competenze necessarie per rafforzare la sicurezza dei sistemi informatici e mitigare il rischio di attacchi informatici.

Obiettivi del corso:

CYBER DEFENSE È

Un percorso strutturato con l'obiettivo di supportare i corsisti nella gestione della Sicurezza Informatica.

GLI OBIETTIVI

- Conoscenza è difesa: impara a conoscere le minacce che mettono a rischio la tua organizzazione.
- Resilienza: padroneggia le best practice e gli strumenti per difendere il tuo perimetro digitale.
- Il fattore umano: la Cyber non è solo tecnologia, proteggerà i tuoi dipendenti.
- Vai oltre la superficie: approfondisci la Threat Intelligence e conosci il dark web.
- Costruisci la sicurezza: come impostare un framework efficace ed efficiente.
- Worst case scenario: scegli come affrontare un Data Breach.

Sei punti fondamentali, un percorso completo ed esaustivo per comprendere i rischi, riconoscerli e contrastarli in maniera efficace.

Argomenti trattati:

Partner tecnico

[Swascan](#) è una Cyber Security Company nata da un'idea di Pierguido Iezzi e Raoul Chiesa. È la prima azienda di Cyber Security Italiana proprietaria di una piattaforma di Cyber Security Testing e Threat Intelligence, oltre ad essere un centro di eccellenza di Cyber Security Research. Swascan è stata premiata con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo. Da ottobre 2020, Swascan srl è parte integrante di Tinexta Cyber (Tinexta S.P.A), diventando protagonista attiva del primo polo nazionale di Cyber Security: non solo un'azienda, dunque, ma un gruppo italiano e un hub nazionale specializzato nei servizi di identità digitale e sicurezza digitale.

Destinatari:

Il corso si rivolge a tutti coloro che vogliono acquisire conoscenze, metodologie e strumenti per la gestione e la tutela del perimetro aziendale e dei dati sensibili.

Tra i principali professionisti:

- Personale IT e ICT
- Responsabili Cyber Security
- Auditor
- DPO
- Legal Office
- CEO, CISO, CSO, CIO
- Decision Maker e Impreditori

Le caratteristiche e il taglio formativo particolarmente innovativo ed efficace rendono il percorso adatto anche a Studenti di Ingegneria, Informatica, e Computer Science per integrare il loro curriculum accademico con nozioni, concetti ed esercitazioni pratiche nonché e a tutti coloro che sono appassionati di Cyber Security e vorrebbero arricchire il proprio bagaglio personale.