


CPENT – CERTIFIED PENETRATION TESTING PROFESSIONAL v1

Descrizione	<p>Corso tecnico-pratico ufficiale EC-Council di certificazione Certified Penetration Testing Professional (CPENT v.1), per professionisti della sicurezza informatica esperti, finalizzato a eseguire un Penetration test efficace in un ambiente di rete.</p> <p>I laboratori replicano una rete aziendale accurata per un apprendimento pratico come dal vivo. Vi sono diversi livelli di segmentazione della rete e il corso insegna come navigare liberamente tra questi livelli attraverso azioni di Pen Testing</p> <div style="text-align: right;">  </div>
Obiettivi	<ul style="list-style-type: none"> Eseguire tecniche e attacchi avanzati per identificare le vulnerabilità SQL injection, Cross site scripting (XSS), LFI, RFI nelle applicazioni web Scrivere codici di exploit (sfruttamento binario avanzato) per ottenere l'accesso a un sistema o un'applicazione vulnerabile Sfruttare le vulnerabilità nei sistemi operativi come Windows, Linux Attaccare sistemi IoT e quindi ottenere accesso alla rete Eseguire l'escalation dei privilegi per ottenere l'accesso root a un sistema Pentesting Operational Technology (OT), attraverso reti SCADA ICS Accedere a reti nascosti con Pivoting e Double Pivoting Redigere un report professionale Dimostrare un pensiero "fuori dagli schemi" e "laterale"
Vantaggi	<ul style="list-style-type: none"> Mappato al framework NICE Combina approcci di Pen Testing manuali e automatizzati Attività di laboratorio dinamiche e sempre aggiornate
Programma di dettaglio	<ul style="list-style-type: none"> Introduction to Penetration Testing Penetration Testing Scoping and Engagement Open Source Intelligence (OSINT) Social Engineering Penetration Testing Network Penetration Testing – External Network Penetration Testing– Internal Network Penetration Testing – Perimeter Devices Web Application Penetration Testing Wireless Penetration Testing IoT Penetration Testing OT/SCADA Penetration Testing Cloud Penetration Testing Binary Analysis and Exploitation Report Writing and Post Testing Actions
Destinatari	Penetration Tester, Security Analyst, etc.
Pre-requisiti	<p>Conoscenza di:</p> <ul style="list-style-type: none"> Sistemi Operativi (Linux, Windows, Mac OSX, Android, iOS) Reti dati (TCP/IP, protocollo UDP, modello ISO/OSI, protocolli applicativi) Sistemi di virtualizzazione Concetti di programmazione Fondamenti di Sicurezza informatica Inglese tecnico scritto (il corso è tenuto in italiano, materiali didattici ed esami sono in lingua inglese) <p>È fortemente raccomandato aver già conseguito la certificazione CEH (Certified Ethical Hacker)</p>

CPENT – CERTIFIED PENETRATION TESTING PROFESSIONAL v1

<p>Durata e frequenza</p>	<p>Corso della durata di 5+1 giornate (ciascuna tra le 9:00 e le 18:00, comprese pause). La sesta giornata è offerta come ripasso complessivo e preparazione all'esame di certificazione. L'esame di certificazione si tiene online in giornate a parte.</p> <p><i>Assenze superiori alle 4 ore consecutive pregiudicano le competenze acquisite e possono compromettere il risultato dell'esame finale.</i> <i>Si raccomanda di prevedere del tempo individuale aggiuntivo per consolidare l'apprendimento (attività individuali post-aula, riguardare o completare le esercitazioni e riesaminare la documentazione).</i></p>
<p>Modalità di partecipazione</p>	<ul style="list-style-type: none"> • In presenza in aula con docente • (eccezionalmente) In Virtual Classroom: in web-conference connessi in tempo reale dal proprio dispositivo con il docente e gli altri allievi • In ASA (Autoformazione Specialistica Assistita): autoformazione con incontri individuali con il docente • In aula remota: con gruppi di allievi distribuiti, live, su più aule fisiche, connesse in web-conference tra loro e con il docente • In e-learning: autoformazione con accesso individuale autenticato ai materiali interattivi <p><i>È anche possibile alternare le precedenti modalità</i></p>
<p>Profilo Docenti</p>	<p>Docenti, consulenti e formatori ICT esperti e specializzati sui Sistemi Informatici, certificati CEH e CPENT e abilitati come Certified EC-Council Instructor (CEI).</p> <p><i>Competenze e certificazioni dei docenti possono essere verificate prima dell'inizio del corso, a garanzia del valore aggiunto e del livello qualitativo dei contenuti.</i></p>
<p>Metodologia</p>	<p>Per raggiungere alti livelli di apprendimento, vengono integrate diverse metodologie didattiche, in aggiunta alla programmazione, alla qualità dei materiali didattici, e alla professionalità dei docenti:</p> <ul style="list-style-type: none"> • Learning by doing: imparare facendo. È la metodologia principalmente utilizzata per i corsi abilitanti, integrata dall'uso di supporti didattici di varia natura e dal coinvolgimento immediato dei discenti • Learning Experience: acquisire competenze pratiche attraverso le attività tecnico pratico e l'esperienza sul campo dei formatoti • Participatory Learning: massimizzare l'apprendimento attraverso la partecipazione attiva, l'interazione con i colleghi, i lavori di gruppo, le attività collaborative <p>Le metodologie includono:</p> <ul style="list-style-type: none"> • Lezioni frontali interattive con i docenti • Alternanza di sessioni teoriche e pratiche • Materiali didattici (ufficiali EC-Council) di elevata qualità; in inglese, accessibile h24 per 2 anni • Laboratori remoti (ufficiali EC-Council) disponibili h24 per 6 mesi • Piattaforme e-learning accessibili anche fuori orario di lezione • Studio di situazioni e casi reali • Momenti di knowledge sharing • Monitoraggio dell'apprendimento • Coaching, Mentoring, Tutoraggio individuale e d'aula • Profilazione attitudinale e orientamento professionale • Forum e/o chat di discussione tra allievi anche fuori orario di lezione • Questionario di gradimento
<p>Materiali didattici</p>	<p>Distribuiti in formato elettronico, tramite piattaforme e-learning ufficiali EC-Council, con accesso individuale autenticato:</p> <ul style="list-style-type: none"> • Slide proiettate durante il corso • Dispense • Materiale integrativo • Laboratori ed esercitazioni • Voucher per esame di certificazione CPENT (attivo 1 anno) <p><i>Si raccomanda di organizzarsi per portarsi in aula i materiali didattici o su proprio</i></p>

CPENT – CERTIFIED PENETRATION TESTING PROFESSIONAL v1

	<p>supporto elettronico (notebook, Tablet, Smartphone).</p>
<p>Esame di certificazione</p>	<p>Al termine del corso viene rilasciato un voucher d'esame della validità di 1 anno dall'attivazione per sostenere l'esame di certificazione CPENT – Certified Penetration Testing Professional.</p> <p>L'esame si tiene online con una supervisione remota da parte di EC-Council.</p> <p>Si tratta di un esame pratico, composto da 10 challenge + Report Writing, della durata di 24 ore totali (è possibile suddividere l'esame in due da 12 ore).</p> <p>La soglia di superamento è del 70%; ottenendo un punteggio superiore al 90% si ottiene anche la prestigiosa certificazione LTP Master.</p>
<p>Attestato e Certificazione</p>	<ul style="list-style-type: none"> • A termine del corso viene rilasciato un attestato di frequenza EC-COUNCIL-ITHUM • Al superamento dell'esame di certificazione, si ottiene l'Attestato di certificazione CPENT – Certified Penetration Testing Professional Hacker
<p>Allestimento d'aula (Corsi in presenza)</p>	<p>Aule adeguate e confortevoli per svolgere attività didattiche, dotate di:</p> <ul style="list-style-type: none"> • Accesso a Internet • Sistema di videoproiezione • Lavagna a fogli mobili e/o white-board, con pennarelli colorati • Tavoli e sedie mobili (non sedie con ribaltine o bloccate in configurazioni fisse) • Climatizzazione e areazione adeguata • Raggiungibilità con trasporti pubblici
<p>A cura degli allievi</p>	<p>Notebook personale con accesso amministratore</p>
<p>Numero partecipanti</p>	<p>Fino a 15 allievi per edizione (<i>per ottimizzare l'efficacia dell'interazione e dell'apprendimento</i>)</p>
<p>Altri corsi EC-Council</p>	<p>In qualità di partner EC-Council, ITHUM eroga anche i corsi di certificazione, tra cui:</p> <ul style="list-style-type: none"> • CEH - Certified Ethical Hacker • CND - Certified Network Defender • CHFI - Certified Hacking Forensic Investigator • CSA - Certified SOC Analyst • ECIH - EC-Council Certified Incident Handler • CTIA - Certified Threat Intelligence Analyst
<p>Informazioni e prenotazioni</p>	<ul style="list-style-type: none"> • Mail: formazione@ithum.it • Telefono: (+39) 06 2158915 • Sito: https://www.ithum.it/formazione/cybersec/ec-council-corsi-e-certificazioni.html