OpenCertif
Centre de formation et de certification professionnelle

SYLLABUS OFFICIEL

Examen CEH 312-50

Certified Ethical Hacker (CEH v13)
Analyse, pentest et sécurité offensive

Certification : Certified Ethical Hacker (CEH)

Niveau : Intermédiaire / Avancé | Public : Pentesters / Analystes SOC / Consultants cybersécurité

1. Présentation de la certification

L'examen **Certified Ethical Hacker (CEH) 312-50**, délivré par **EC-Council**, est la certification mondiale de référence en **ethical hacking et sécurité offensive**. Elle valide votre capacité à **identifier, exploiter et corriger des vulnérabilités** dans des environnements réseau, système et applicatif, tout en respectant une approche éthique et réglementée. La devise CEH : "*To beat a hacker, you need to think like a hacker*".

La version actuelle **CEH v13** intègre l'**IA dans les 5 phases de l'ethical hacking** (reconnaissance, scanning, gaining access, maintaining access, covering tracks) avec une promesse de **10x d'efficacité** dans le travail de cybersécurité. L'examen comporte **20 modules couvrant l'ensemble de la méthodologie d'ethical hacking**. Passé via Pearson VUE ou en centre EC-Council agréé. Note : **OpenCertif est un centre Pearson VUE Authorized Test Center** et peut héberger l'examen.

Informations clés

Code de l'examen	312-50 (Certified Ethical Hacker)
Intitulé officiel	Certified Ethical Hacker (CEH v13)
Certification obtenue	Certified Ethical Hacker — EC-Council
Éditeur officiel	EC-Council (International Council of E-Commerce Consultants)
Centre de test	Pearson VUE (OpenCertif est Authorized Test Center) ou centre EC-Council agréé
Version actuelle	CEH v13 (avec intégration IA dans les 5 phases d'ethical hacking)
Nombre de modules	20 modules officiels couvrant toute la méthodologie
Format	QCM supervisé (en ligne ou en centre)
Durée de l'examen	4 heures (240 minutes)
Nombre de questions	125 questions à choix multiple
Score requis	Variable de **60 % à 85 %** selon la difficulté du pool de questions (cut score adaptatif EC-Council)
Langue de l'examen	Anglais (langue principale)

Prérequis recommandé	2 ans d'expérience en sécurité IT minimum (recommandation EC-Council). TCP/IP, OS Windows/Linux et scripting Python/Bash facilitent la réussite.
Prérequis formel	Soit suivre la **formation officielle EC-Council CEH**, soit soumettre un **eligibility form** avec preuve de 2 ans d'expérience.
Formules OpenCertif	**Cours en ligne** | **Bon d'examen seul** | **Pack complet** (Cours + Labs CEH Engage + Examen 312-50)
Tarif voucher	Environ 650 € à 1 199 € (voucher seul EC-Council)
Validité de la certification	3 ans — renouvellement par **120 ECE credits** ou en repassant le dernier examen CEH
Badge numérique	Badge officiel EC-Council délivré via Credly
Conformité	**DoD 8570/8140** (Département de la Défense US)

2. Profil du candidat

En tant que candidat à l'examen CEH 312-50, vous développez et validez des compétences professionnelles en ethical hacking et sécurité offensive. Vous êtes capable de :

- Comprendre les concepts fondamentaux de la sécurité de l'information.
- Connaitre les **lois et réglementations** applicables (GDPR, cyber laws, privacy acts).
- Effectuer du **footprinting** et de la reconnaissance passive et active.
- Scanner les réseaux avec Nmap et identifier les services exposés.
- Effectuer de l'**enumeration** via SMB, SNMP, LDAP, NetBIOS.
- Conduire une **vulnerability assessment** avec Nessus, OpenVAS.
- Exploiter les systèmes via **Metasploit** et techniques d'escalade de privilèges.
- Créer et analyser les **malware** : virus, trojans, worms, ransomware.
- Effectuer du **sniffing** avec Wireshark et analyser les protocoles réseau.
- Réaliser des attaques de **social engineering** (phishing, vishing, pretexting).
- Comprendre et reproduire des attaques **DoS / DDoS**.
- Effectuer du **session hijacking** et man-in-the-middle.
- Évader les IDS, firewalls et honeypots.
- Auditer la sécurité des **serveurs web** et **applications web**.
- Exploiter les **injections SQL**, **XSS**, **CSRF** et autres vulnérabilités OWASP Top 10.
- Auditer les réseaux **WiFi** et casser les protocoles WEP/WPA/WPA2/WPA3.
- Pentester les plateformes mobiles **Android** et **iOS**.
- Auditer la sécurité des dispositifs **IoT** et environnements **OT** (industriel).
- Auditer la sécurité des environnements **cloud** (AWS, Azure, GCP).
- Comprendre et utiliser la **cryptographie** : symétrique, asymétrique, hashing.
- Utiliser l'**IA pour renforcer chaque phase** d'ethical hacking (CEH v13).
- Rédiger un **rapport d'audit** structuré et actionnable.

L'examen évalue spécifiquement cinq familles de compétences correspondant aux **5 phases d'ethical hacking** reconnues par EC-Council (et listées par OpenCertif) :

- Techniques de reconnaissance et collecte d'informations.
- Analyse des vulnérabilités et évaluation des risques.
- Exploitation des failles réseau, système et applicatives.
- Post-exploitation, escalade de privilèges et maintien d'accès.
- Contre-mesures, durcissement et rédaction de rapports d'audit.

3. Prérequis et public cible OpenCertif

EC-Council recommande aux candidats de disposer de :

- **2 ans ou plus d'expérience en sécurité IT** (recommandation officielle EC-Council).
- Soit avoir suivi la **formation officielle EC-Council CEH** (iLearn, iClass ou via partenaire agréé), soit avoir soumis un **eligibility form** avec preuve d'expérience.
- Solide compréhension de **TCP/IP** et des protocoles réseau (HTTP, DNS, DHCP, ARP).

- Connaissance des systèmes d'exploitation **Windows et Linux** (commandes shell, services).
- Familiarité avec les services réseau courants (HTTP, FTP, SSH, SMB, RDP).
- **Scripting Python ou Bash** est très utile (lecture et adaptation de scripts d'exploit).
- Certifications pré-requises souvent utiles : **CompTIA Network+** et **Security+**.
- Accès à un laboratoire Kali Linux pour la pratique (machine virtuelle ou physique).
- Anglais niveau intermediaire/avancé (l'examen est exclusivement en anglais).
- **Optionnel mais recommandé** : passer les certifications EC-Council Essentials (EHE, DFE, CSE) avant le CEH — OpenCertif propose ce parcours d'initiation progressif.

Public cible OpenCertif

- **Pentesters juniors et seniors** souhaitant valider leurs compétences offensives.
- **Analystes SOC** (Security Operations Center) niveau 1, 2 et 3.
- **Administrateurs réseau et système** en évolution vers la cybersécurité.
- **Consultants cybersécurité** en agence ou en interne.
- **Auditeurs sécurité** et analystes vulnérabilités.
- **Red Team operators** et professionnels en offensive security.
- **Officers sécurité IT** (CISO juniors, responsables sécurité SI).
- Étudiants en cybersécurité (Bachelor, Master) souhaitant un premier emploi pentester.
- Profils en reconversion vers le métier de l'ethical hacking.
- Forces de l'ordre et personnel des forces armées (CEH conforme DoD 8570/8140).
- Profils ayant suivi les EC-Council Essentials (**EHE, DFE, CSE**) sur OpenCertif.
- Candidats aux certifications avancées EC-Council : **CEH Practical**, **CPENT**, **LPT Master**.

4. Domaines de compétences mesurées

L'examen est structuré autour de 5 grands domaines de compétences. Le tableau ci-dessous indique le poids relatif de chaque domaine dans l'évaluation finale (version 2026 — aligné sur CEH v13 / 312-50 avec intégration IA). Les pondérations sont des estimations issues du guide officiel Unity / Certiport.

Domaine	Intitulé	Pondération
1	Reconnaissance et collecte d'informations	20 — 25 %
2	Analyse des vulnérabilités et évaluation des risques	15 — 20 %
3	Exploitation des failles réseau, système et applicatives	30 — 35 %
4	Post-exploitation, escalade de privilèges et maintien d'accès	15 — 20 %
5	Contre-mesures, durcissement et reporting	10 — 15 %

*Remarque : l'examen UCU Programmer dure environ 50 minutes pour 40 questions, soit environ 1 minute 15 par question. La gestion du temps est essentielle. Le score requis pour valider est de **500 sur 700** (sur une échelle officielle Unity de 200 à 700 points).*

5. Détail des compétences mesurées

Cette section détaille de manière exhaustive l'ensemble des compétences couvertes par l'examen CEH 312-50, en s'appuyant sur les Objective Domains publiés par Certiport et Unity Technologies (version 2026 — aligné sur CEH v13 / 312-50 avec intégration IA).

1 Reconnaissance et collecte d'informations — 20 — 25 %

1.1 Fondamentaux de l'ethical hacking

- Concepts de cybersécurité : CIA Triad (Confidentiality, Integrity, Availability).
- Types de hackers : **White Hat**, Black Hat, Gray Hat, Script Kiddie, Hacktivist.
- Les **5 phases d'ethical hacking** : Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks.
- Cyber Kill Chain Methodology (Lockheed Martin) et MITRE ATT&CK; Framework.
- Lois et compliance : **RGPD**, cyber laws France/UE, Wassenaar Arrangement.
- Code d'éthique EC-Council et règles d'engagement (Rules of Engagement).

1.2 Footprinting et reconnaissance passive

- **OSINT** (Open Source Intelligence) : Google Dorks, Shodan, Maltego, theHarvester.
- Footprinting via moteurs de recherche, réseaux sociaux, sites web.
- WHOIS, DNS interrogation, DNSdumpster, dig, nslookup.
- Email tracking, banner grabbing passif.
- Recoltes d'informations sur les **collaborateurs cibles** (LinkedIn, Twitter). pour préparer le social engineering.
- Contre-mesures de footprinting : informations limitées publiques, anti-OSINT.

1.3 Scanning Networks

- Types de scans Nmap : **-sS (SYN stealth)**, -sT (TCP connect), -sU (UDP), -sV (version), -O (OS fingerprinting), -A (aggressive).
- Ping sweeps, port scans, version detection, banner grabbing actif.
- Network mapping et topology discovery.
- Proxy chains et anonymisation (Tor, proxychains).
- Contre-mesures : IDS / IPS, firewall rules, rate-limiting.

1.4 Enumeration

- **NetBIOS / SMB enumeration** : enum4linux, smbclient, rpcclient.
- **SNMP enumeration** : snmpwalk, default community strings.
- **LDAP enumeration** : ldapsearch, JXplorer.
- **NFS enumeration** : showmount, NFS exploits.
- **BGP enumeration** et SMTP user enumeration.
- DNS zone transfers et Active Directory enumeration (PowerView, BloodHound).

2 Analyse des vulnérabilités et évaluation des risques — 15 — 20 %

2.1 Vulnerability Assessment

- Méthodologies d'assessment : Active vs Passive, Internal vs External.
- Outils : **Nessus**, **OpenVAS**, Qualys, Nikto, Acunetix.
- Scoring : **CVSS** (Common Vulnerability Scoring System).
- Bases de données : **CVE**, **NVD**, Exploit-DB, Vulners.

2.2 Types de vulnérabilités

- Vulnérabilités système : misconfigurations, default credentials, unpatched.
- Vulnérabilités réseau : services obsolètes, protocoles faibles.
- Vulnérabilités applicatives : **OWASP Top 10**.
- Zero-days et N-days, exploitabilité et impact.

2.3 Évaluation des risques

- Risk = Threat × Vulnerability × Asset Value.
- Methodologies : **OCTAVE**, **FAIR**, NIST RMF.
- Prioritization : matrices de risque, heat maps.
- Rédaction des findings dans le rapport d'audit.

3 Exploitation des failles réseau, système et applicatives — 30 — 35 %

3.1 System Hacking et exploitation

- **Password attacks** : dictionary, brute force, rainbow tables, password spraying.
- Outils : **Hashcat**, John the Ripper, Hydra, Medusa.
- Pass-the-Hash, Pass-the-Ticket (Kerberos).
- **Metasploit Framework** : msfconsole, search, use, set options, exploit.
- Exploit development basics : buffer overflow, ROP chains (notions).

3.2 Malware et menaces

- Types de malware : **Virus**, **Trojan**, **Worm**, **Ransomware**, RAT, Rootkit, Keylogger.
- Création et analyse de malware basique avec **msfvenom**.
- Techniques d'obfuscation, packing, encoding pour évader les AV.
- Analyse dynamique et statique de malware (sandbox, IDA, Ghidra).
- APTs (Advanced Persistent Threats) et techniques associées.

3.3 Sniffing et man-in-the-middle

- **Wireshark** : display filters, capture filters, analyse de protocoles.
- tcpdump et capture en CLI.
- ARP spoofing avec **arpspoof**, ettercap, Bettercap.
- DNS spoofing, DHCP spoofing.
- SSL stripping et HTTPS interception (sslstrip).

3.4 Social Engineering

- Techniques : **phishing**, vishing (voice), smishing (SMS), pretexting.
- Frameworks : **SET** (Social-Engineer Toolkit), Gophish.
- Spear phishing et BEC (Business Email Compromise).
- Physical social engineering : tailgating, badge cloning, dumpster diving.
- Contre-mesures : awareness training, MFA, email filtering.

3.5 Attaques sur applications web

- **OWASP Top 10** : Injection, Broken Authentication, XSS, Insecure Deserialization, etc.
- **SQL Injection** : Union-based, Boolean-based, Time-based, Out-of-band.
- Outils : **SQLmap**, **Burp Suite**, OWASP ZAP.
- **XSS** (Stored, Reflected, DOM-based) et CSRF.
- **File Upload vulnerabilities**, Local File Inclusion (LFI), Remote File Inclusion (RFI).
- Command injection, XXE, SSRF.
- Hacking de Web Servers : Apache, Nginx, IIS et leurs vulnérabilités.

3.6 Attaques DoS / DDoS

- Types d'attaques : Volumetric (UDP flood, ICMP flood), Protocol (SYN flood), Application Layer.
- Botnets : Mirai, Emotet, et command-and-control (C2) infrastructure.
- Amplification attacks : DNS, NTP, Memcached.
- Contre-mesures : rate limiting, CDN, WAF, DDoS mitigation (Cloudflare, Akamai).

3.7 Wireless, mobile, IoT et cloud

- **Wireless** : WEP, WPA, WPA2, WPA3 cracking avec aircrack-ng, Wifite.
- Evil Twin, Karma attack, deauthentication attacks.
- **Mobile (Android/iOS)** : reverse engineering APK, jailbreaking, root, Frida, MobSF.
- **IoT/OT** : MQTT, Modbus, ICS/SCADA security.
- **Cloud** : AWS S3 misconfigurations, IAM, Azure AD, GCP, conteneurs Docker/Kubernetes.

4 Post-exploitation, escalade de privilèges et maintien d'accès — 15 — 20 %

4.1 Privilege escalation

- **Windows privilege escalation** : kernel exploits, DLL hijacking, unquoted service paths.
- **Linux privilege escalation** : SUID binaries, sudo misconfigurations, cron jobs, kernel.
- Outils : **WinPEAS**, **LinPEAS**, **BloodHound** (Active Directory).
- Token impersonation, Kerberoasting, AS-REP Roasting.

4.2 Maintaining access et persistence

- **Backdoors** : Netcat reverse shells, Meterpreter persistence.
- **Rootkits** : kernel-mode et user-mode rootkits.
- Persistence Windows : registry run keys, scheduled tasks, services, WMI.
- Persistence Linux : cron, systemd services, .bashrc, SUID backdoors.

4.3 Session Hijacking

- Network-level hijacking : TCP/IP session hijacking.
- Application-level hijacking : session token theft, cookie hijacking.
- Cross-Site Script Inclusion (XSSI), Session Fixation.
- Tools : **Burp Suite**, OWASP ZAP, Hetty.

4.4 Évasion IDS / firewalls / honeypots

- Techniques d'évasion : fragmentation IP, encryption, encoding, timing manipulation.
- **Snort** et Suricata : signatures et bypass.
- Firewall evasion : source port manipulation, packet crafting (hping3, Scapy).
- Identification et bypass des **honeypots**.

4.5 Cleaning tracks

- Effacement des logs Windows (Event Viewer, evtutil clear) et Linux (auth.log, syslog).
- Anti-forensics : timestomping, secure delete, log tampering.
- Aspects éthiques et légaux — ce que CEH enseigne dans le cadre légal de pentests autorisés.

5 Contre-mesures, durcissement et reporting — 10 — 15 %

5.1 Cryptographie

- **Symétrique** : AES, DES, 3DES, ChaCha20, modes (CBC, GCM, ECB).
- **Asymétrique** : RSA, ECC, Diffie-Hellman, ECDSA.
- **Hashing** : SHA-256, SHA-3, bcrypt, Argon2, MD5 (faible).
- PKI, certificats X.509, TLS/SSL, OpenSSL.
- Attaques cryptographiques : birthday attack, padding oracle, length extension.
- Steganographie : Steghide, OpenStego.

5.2 Durcissement et défense

- **Hardening** Windows, Linux et réseau (CIS Benchmarks).
- Patch management et vulnerability management lifecycle.
- **Defense in Depth** : couches multiples (network, host, app, data).
- SIEM : Splunk, ELK Stack, QRadar.
- Zero Trust Architecture et microsegmentation.

5.3 Rapport d'audit pentest

- Structure d'un rapport : Executive Summary, Methodology, Findings, Recommendations.
- Classification des findings : Critical, High, Medium, Low, Informational.
- Reproduction des vulnérabilités avec PoC (Proof of Concept) sans causer de dommages.
- Recommandations de remediation actionables.
- Frameworks de reporting : PTES (Penetration Testing Execution Standard), OWASP Testing Guide.

5.4 IA et ethical hacking (nouveauté CEH v13)

- Utilisation de l'**IA dans les 5 phases** d'ethical hacking (gain 10x d'efficacité).
- Outils IA pour reconnaissance, scanning, exploitation.
- Attaques sur les **systèmes IA** : prompt injection, model poisoning, adversarial attacks.
- Défense des systèmes IA contre les attaques.

6. Modalités pédagogiques OpenCertif

OpenCertif accompagne les candidats au CEH 312-50 à travers un parcours blended-learning complet, combinant ressources e-learning interactives, projets pratiques en Nmap, Wireshark, Metasploit, Burp Suite, OWASP Top 10, Kali Linux, scanning, exploitation et cryptographie et accompagnement tutoré.

Format de la formation

Durée recommandée	200 à 300 heures (OpenCertif propose 3 formules : **cours en ligne**, **bon d'examen seul**, ou **pack complet** avec cours + labs + examen). EC-Council recommande 5 jours en bootcamp intensif ou 8 à 12 semaines en auto-formation (2 à 3 heures par jour)
Modalité	100 % distanciel asynchrone, ou blended (distanciel + classes virtuelles)
Support pédagogique	Unity Certified User Courseware officiel (GMetrix) + ressources OpenCertif (modules Rise 360, scénarios immersifs)
Plateforme LMS	lmsopencertif.fr (Moodle) — accès 24/7 pendant 12 mois
Encadrement	Tutorat asynchrone par expert Unity certifié + classes virtuelles bimensuelles
Pratique requise	Au moins 150 heures de pratique Unity (recommandation officielle Unity Technologies)
Évaluations	Quiz formatifs par module, 3 projets pratiques Unity, examens blancs CertPREP
Certification finale	Passage de l'examen CEH 312-50 en centre OpenCertif (CATC Certiport)

Parcours d'apprentissage proposé

- **Module 1 :** Introduction to Ethical Hacking — concepts, lois, code éthique.
- **Module 2 :** Footprinting and Reconnaissance — OSINT, WHOIS, DNS, theHarvester.
- **Module 3 :** Scanning Networks — Nmap, Hping3, banner grabbing.
- **Module 4 :** Enumeration — SMB, SNMP, LDAP, NetBIOS, NFS, BGP.
- **Module 5 :** Vulnerability Analysis — Nessus, OpenVAS, CVSS, CVE.
- **Module 6 :** System Hacking — password attacks, Metasploit, privilege escalation.
- **Module 7 :** Malware Threats — virus, trojan, ransomware, msfvenom.
- **Module 8 :** Sniffing — Wireshark, ARP spoofing, MITM, sslstrip.

- **Module 9 :** Social Engineering — phishing, SET, Gophish, BEC.
- **Module 10 :** Denial-of-Service — DDoS, botnets, amplification, mitigation.
- **Module 11 :** Session Hijacking — TCP, cookies, Burp Suite, OWASP ZAP.
- **Module 12 :** Evading IDS, Firewalls, and Honeypots — fragmentation, packet crafting.
- **Module 13 :** Hacking Web Servers — Apache, Nginx, IIS vulnerabilities.
- **Module 14 :** Hacking Web Applications — OWASP Top 10, XSS, CSRF, file upload.
- **Module 15 :** SQL Injection — SQLmap, Union, Boolean, Time-based, Out-of-band.
- **Module 16 :** Hacking Wireless Networks — WEP, WPA/WPA2/WPA3, aircrack-ng, Evil Twin.
- **Module 17 :** Hacking Mobile Platforms — Android, iOS, Frida, MobSF.
- **Module 18 :** IoT and OT Hacking — MQTT, Modbus, ICS/SCADA.
- **Module 19 :** Cloud Computing — AWS, Azure, GCP, conteneurs Docker/Kubernetes.
- **Module 20 :** Cryptography — AES, RSA, hashing, PKI, attaques cryptographiques.
- **Pratique CEH Engage :** 4 phases d’emulated ethical hacking engagement sur cible réelle.
- **Examen blanc CEH 312-50** et révision avant le passage à Pearson VUE.

7. Ressources d’étude officielles

En complément du parcours OpenCertif, les ressources officielles Unity Technologies et Certiport suivantes sont fortement recommandées :

- Site officiel EC-Council : **eccouncil.org/train-certify/certified-ethical-hacker-ceh**.
- EC-Council iLearn et iClass (cours officiel CEH avec labs CEH Engage).
- CEH Engage : 4-phase emulated ethical hacking engagement (nouveau v13).
- EC-Council CodeRed : plateforme de cours complémentaires.
- Documentation officielle : **CEH Exam Blueprint v13** (PDF EC-Council).
- Practice tests : **EC-Council Aspen portal**, Boson, MeasureUp.
- Plateformes de practice : **TryHackMe** (Pre-Security, CEH Path), **Hack The Box**, OverTheWire.
- OWASP Top 10 : **owasp.org/Top10** — référence pour les vulnérabilités web.
- MITRE ATT&CK; Framework : **attack.mitre.org**.
- Distribution offensive : **Kali Linux** (kali.org) et Parrot OS.
- Documentation Metasploit (rapid7.com/products/metasploit) et Nmap (nmap.org).
- Page Pearson VUE : **home.pearsonvue.com/eccouncil**.
- OpenCertif est **Pearson VUE Authorized Test Center** et peut accueillir l’examen CEH.
- Page officielle OpenCertif : **opencertif.fr/ec-council/ceh**.
- Badge officiel délivré via Credly (credly.com).
- Communauté EC-Council et forums Reddit (r/CEH, r/cybersecurity).

8. Modalités de passage de l’examen

Inscription	Via OpenCertif ou directement auprès d’un centre Certiport
Centre d’examen	OpenCertif — Centre Certiport Authorized Testing Center (CATC) / Pearson VUE
Mode de passage	En centre uniquement (Unity n’autorise pas l’examen OnVUE à distance pour les certifications UCU — présence sur site requise)
Pièce d’identité	1 pièce d’identité avec photo obligatoire le jour de l’examen (pour les mineurs : autorisation parentale et CNI / passeport)
Aménagements	Demande possible auprès de Certiport (temps additionnel, assistance technique)

Résultat	Score communiqué immédiatement à la fin de l'examen (échelle 200-700, seuil de réussite 500)
Validité de la certification	3 ans à partir de la date de réussite — attribuée une seule fois (stackable, pas de renouvellement payant requis)
Politique de reprise	Délai d'attente de 24 heures avant la 1re reprise. Voucher retake à utiliser sous 60 jours après l'échec.
Badge numérique	Badge officiel délivré via Credly et intégrable à LinkedIn, CV, portfolio, sites de recrutement

9. Contact et inscription

Pour toute information complémentaire, demande de devis ou inscription à la formation préparatoire au CEH 312-50, l'équipe OpenCertif reste à votre disposition. OpenCertif est un Centre Certiport Authorized Testing Center (CATC) habilité à délivrer les certifications Unity Certified User.

OpenCertif
Centre de formation et de certification

app.opencertif.fr
lmsopencertif.fr

Centre agréé Certiport / Pearson VUE
Certifié Qualiopi — Actions de formation

10. Mentions légales et version

Ce syllabus est établi par OpenCertif sur la base des Objective Domains officiels publiés par Certiport pour la certification CEH 312-50, dans sa version applicable (version 2026 — aligné sur CEH v13 / 312-50 avec intégration IA). Les compétences mesurées, les pondérations et les objectifs présentés reflètent fidèlement la structure de l'examen telle que publiée par Unity Technologies via Certiport.

Version du syllabus : 2026.05 — Édition mai 2026
Source officielle Certiport : certiport.pearsonvue.com/Certifications/Unity/Certified-User/Certify
Source officielle Unity : unity.com/products/unity-certifications/user-programmer

Page OpenCertif : opencertif.fr/unity-user-programmer