+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 11/04/2024

S'inscrire

Formation Certification Comptia Pentest+© (PT0-002)

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Notre formation Comptia Pentest+© vous préparera efficacement au passage de la certification. Cette certification vous permettra de prouver vos compétences en test d'intrusion et en sécurité informatique, renforçant ainsi votre crédibilité et votre valeur sur le marché professionnel.

Notre programme de cours couvre divers modules, dont la planification et l'étendue des tests, la collecte d'informations et le balayage des vulnérabilités, les attaques et exploits, la communication des rapports, ainsi que l'utilisation des outils et l'analyse de code.

Notre formation vous prépare à réussir l'examen en vous fournissant des connaissances approfondies sur les concepts de gouvernance, les réglementations en matière de conformité, les méthodes d'attaque, et les meilleures pratiques en matière de test d'intrusion.

Nous mettons constamment à jour notre programme pour refléter les dernières évolutions de l'industrie et assurer que nos apprenants disposent des compétences les plus récentes.

Objectifs

- Acquérir une compréhension approfondie des exigences de conformité réglementaire
- Maîtriser les concepts de planification et de délimitation du périmètre des tests
- Appliquer les normes et méthodologies reconnues
- Développer des compétences en communication et en rédaction de rapports
- Se familiariser avec une variété d'outils d'analyse de vulnérabilités et de code

Public visé

- Pentesters
- Analystes en cybersécurité
- Consultants en sécurité
- Administrateurs systèmes

Pré-requis

- 3 à 4 ans d'expérience pratique dans la réalisation des tests d'intrusion, des évaluations de vulnérabilité et l'analyse de code
- Connaissances solides en sécurité informatique
- Avoir des notions fondamentales sur les tests d'intrusion
- Connaissances en langages de script comme Python ou Ruby

Pré-requis logiciels

- Environnement de virtualisation (VMware ou VirtualBox)
- Outils de test de vulnérabilité (Nmap, Metasploit, Burp Suite, OWASP ZAP, SQLmap...)
- Outils de gestion de mots de passe et de stockage sécurisé des informations sensibles

Note : Ambient IT n’est pas propriétaire de Comptia Certifications©, cette certification appartient à Comptia®, Inc.

Programme de la Préparation à la Certification Pentest+©

Planning et Scoping (14%)

- Considérations relatives à la conformité réglementaire
  - Payment Card Industry Data
  - Security Standard (PCI DSS)
  - General Data Protection Regulation (GDPR)
- Restrictions de localisation
  - Limitations des pays
  - Restrictions des outils
  - Lois locales
- Legal concepts
  - SLA
  - Confidentialité
  - Non-disclosure agreement (NDA)

- Standards et méthodologie
  - MITRE ATT&CK
  - Open Web Application
  - Security Project (OWASP)
  - National Institute of Standards
  - and Technology (NIST)
  - Open-source Security Testing
  - Methodology Manual (OSSTMM)
  - Penetration Testing
  - Execution Standard (PTES)
  - Information Systems Security
  - Assessment Framework (ISSAF)
- Règles d'engagement
  - Heure de la journée
  - Types de tests autorisés/interdits
  - Autres restrictions
- Considérations environnementales
  - NetworkApplicationCloud
- Target list/in-scope assets
  - Wireless networks
  - Internet Protocol (IP) ranges
  - Domains
  - Application programming interfaces (APIs)
  - Emplacements physiques
  - Domain name system (DNS)
  - External vs. internal targets
  - First-party vs. third-party hosted
- Valider l'étendue de la mission
  - Interroger le client/examiner les contrats
  - Gestion du temps
  - Stratégie
  - Test de l'environnement inconnu vs. tests en environnement connu
- Vérification des antécédents de l'équipe chargée des tests d'intrusion
- Identifier les activités criminelles
- Limiter l'utilisation des outils à une mission particulière
- Maintenir la confidentialité des données/informations

Collecte d'informations et analyse de la vulnérabilité (22%)

- DNS lookups
- Identifier les contacts techniques
- Contacts administrateurs
- Cloud vs. self-hosted
- Scraping réseaux sociaux
- Défauts cryptographiques
- Posture en matière de sécurité
- Data
  - Password dumps
  - Fichiers métadonnées
  - Archivage / Mise en cache de site web
  - Dépôt publics de code source
- OSINT
  - Outils (Shodan, Recon-ng)
  - Sources (CWE, CVE...)

- Reconnaissance site web
  - Crawling
  - Scraping
- Packet crafting (Scapy)
- Defense detection
- Tokens
- Wardriving
- Network traffic
- Cloud asset discovery
- Fingerprinting
- Analyse output from
- Méthodes d'analyse
- Nmap
- Outils de test de vulnérabilité

Attaques et exploits (30%)

- Stress testing pour la disponibilité
- Exploiter les ressources (DB, Packet storm)
- Attaques
  - ARP poisoning
  - Exploit chaining
  - Password attacks
  - On-path (previously knownas man-in-the-middle)
  - Kerberoasting
  - DNS cache poisoning
  - Virtual local area network
  - (VLAN) hopping
  - Network access control (NAC) bypass
  - Media access control (MAC) spoofing
  - Link-Local Multicast Name
  - Resolution (LLMNR)/NetBIOS-
  - Name Service (NBT-NS) poisoning
  - New Technology LAN Manager
  - (NTLM) relay attacks
- Outils (Metasploit, Netcat, Nmap)
- Méthode d'attaques
- Falsification des requêtes côté serveur
- Attacks injections
- Vulnérabilité des applications
- API Attacks
- Directory traversal
- Outils (Web proxies, SQLmap, DirBuster)
- Mobile
  - Vulnérabilités
  - Attaques
  - Outils
- IoT dispositifs
  - BLE attacks
  - Vulnérabilités
- Vulnérabilités des systèmes de stockage de données
- Vulnérabilités de l'interface de gestion
- Vulnérabilités liées aux systèmes de contrôle et d'acquisition de données
  - SCADA
  - IIoT
  - ICS

- Attaques d'ingénierie sociales
- Méthodes d'influence
- Post-exploitation des outils
- Tests de segmentation du réseau
- S'implanter / persister

Rapports et communication (18%)

- Report audience
- Report contenus
- conservation du rapport
- Distribution sécurisée
- Contrôles techniques
  - System hardening
  - Assainissement de l'entrée utilisateur/paramétrer les requêtesImplemented multifactor
  - authentication
  - Encrypt passwords
  - Process-level remediation
  - Patch management
  - Key rotation
- Contrôles administratifs
  - Role-based access control
  - Secure software
  - Cycle de développement
  - Exigences mot de passe
  - Politiques et procédures
- Contrôles opérationnels
  - Job rotation
  - Time-of-day restrictions
  - Mandatory vacations
  - User training
- Contrôles physiques
  - Access control vestibule
  - Biometric controls
  - Video surveillance
- Voie de communication
- Déclencheurs de communication
- Raisons pour la communication
- Redéfinition des priorités des objectifs
- Post-engagement cleanup
- Follow-up actions / retest

Outils et analyse du code (16%)

- Constructions logiques
  - Loops
  - Conditionals
  - Boolean operator
  - String operator
  - Arithmetic operator

- Structures de données
  - JavaScript Object Notation (JSON)
  - Key value
  - Arrays
  - Dictionaries
  - Comma-separated values (CSV)
  - Lists
  - Trees
- Libraries
- Classes
- Procedures
- Functions
- Shells
- Langages de programmation (Python, Ruby, Perl, Javascript)
- Analyse du code
  - Download files
  - Launch remote access
  - Enumerate users
  - Enumerate assets
- Possibilités d'automatisation
  - Automatiser le processus de test d'intrusion
- Scripting pour modifier les adresses IP pendant un test
- Script Nmap pour énumérer les et produire des rapports

Stratégie et méthodes pour réussir l’examen

Examen blanc

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.