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

Mis à jour le 27/06/2024

S'inscrire

Formation certification eLearnSecurity eWPTX©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

3 jours (21 heures)

Présentation

Notre formation de préparation à la certification eWPTX© vous permettra de prouver votre maîtrise des tests de pénétration sur les applications web.

L'examen eWPTX© est basé uniquement sur des compétences pratiques avancées. Ainsi vous pourrez prouver vos compétences en hacking de web apps en situation réelle. Il s'agit d'un examen exigeant où seuls les candidats rédigeant un rapport d'audit de très bon niveau réussissent.

Vous devrez attaquer plusieurs machines dans un lab virtuel. Mais également rédiger un audit de pentesting comprenant une documentation professionnelle ainsi que des recommandations de sécurité. La totale de l'examen est de 14 jours. Il inclut 7 jours d'accès au labs de l'examen ainsi que 7 jours de reaction de votre rapport.

Notre formation préparation à la certification eWPTX© vous présentera tous les éléments nécessaires au passage de l'examen. Les attaques avancées sur les applications web, les injections SQL avancées, ou le cross-site scripting.

Objectifs

- Renforcer ces compétences en pentesting visant les applications web
- Être prêt pour passer la certification eWPTX©

Public visé

- Responsables sécurité
- Auditeurs

- Hackers éthique
- Administrateur réseau

Pré-requis

Bonne expérience en sécurité informatique voir posseder déjà une certification dans le domaine.

Note : Ambient IT n’est pas propriétaire de eWPTX©, cette certification appartient à eLearnSecurity©.

PROGRAMME DE NOTRE FORMATION EWPTX

INTRODUCTION AU PENETRATION TESTING WEB

- Comprendre les bases de la sécurité des applications web et le protocole HTTP
- Vue d'ensemble des vulnérabilités courantes dans les applications web
- Introduction aux outils et techniques de test d'intrusion
- L'importance de l'éthique dans le penetration testing
- Configurer un environnement de test sécurisé

ATTAQUES AVANCÉES SUR LES APPLICATIONS WEB

- Techniques d'exploitation des vulnérabilités XXE et SSRF
- Méthodes d'inclusion de fichiers à distance (RFI) et leurs impacts
- Scénarios pratiques d'attaque et de défense
- Analyse des journaux pour détecter les tentatives d'intrusion
- Utilisation des proxies et des outils d'interception pour manipuler les requêtes web

INJECTION SQL AVANCÉE

- Comprendre les différents types d'injection SQL, y compris l'injection aveugle et hors bande
- Techniques pour identifier les points d'injection SQL dans une application
- Exploiter les vulnérabilités SQL avec des outils automatisés et manuellement
- Études de cas sur les impacts des injections SQL
- Pratiques de mitigation et de sécurisation des bases de données

CROSS-SITE SCRIPTING (XSS) ET ÉVASION DES FILTRES

- Détail des différents types de XSS : Reflected, Stored, et DOM-based
- Techniques avancées d'évasion des filtres XSS et contournement des WAF
- Création et test de scripts XSS pour différentes situations
- Défense contre les attaques XSS : en-têtes HTTP, politiques de sécurité du contenu
- Ateliers pratiques sur l'exploitation et la mitigation XSS

ATTAQUES SUR LA LOGIQUE MÉTIER ET CONTRÔLE D'ACCÈS

- Identification et exploitation des vulnérabilités de la logique métier
- Techniques pour tester et sécuriser les mécanismes d'authentification et de contrôle d'accès
- Exploitation des conditions de course et des vulnérabilités liées aux transactions
- Pratiques de sécurisation des processus d'authentification et de gestion des sessions
- Simulation d'attaques de type énumération de comptes et bypass de contrôles d'accès

DÉFIS CTF (CAPTURE THE FLAG) ET RÉVISION

- Introduction aux compétitions de type Capture The Flag pour la consolidation des acquis
- Mise en place et résolution de défis pratiques couvrant les vulnérabilités étudiées
- Techniques de rédaction de rapports de penetration testing clairs et détaillés
- Session de questions-réponses pour clarifier les doutes et renforcer la compréhension

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.