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

Mis à jour le 10/10/2024

S'inscrire

Formation Certification eLearnSecurity eCPPT©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

4 jours (28 heures)

Présentation

Notre formation de préparation à la certification eCPPT© prouvera vos compétences en pentesting grâce à un examen 100% pratique.

Cet examen en cybersécurité contient les concepts essentiels pour réaliser des tests de pénétration : la compréhension du réseau, des systèmes et des attaques d'applications web.

Il consiste à un test pratique évaluant vos habilités en cyberattaque, mais également vos capacités à fournir un rapport d'audit de pentesting complet.

Notre formation comprend tous les modules présents à l'examen, le programme est ajustable selon vos besoins. Vous réviserez les méthodes de pentesting, les vulnérabilités, les exploitations, le scanning ou encore le développement des exploits.

Vous pourrez ainsi assurer la protection des systèmes informatiques grâce à votre compréhension des méthodes de piratage. Enfin, vous apprendrez les bonnes pratiques pour obtenir la certification grâce aux différents entrainements.

Contenu de la formation

- 6 mois d’accès aux Labs en autoformation
- 4 accompagnements d'expert : 4 jours - 28 heures
- 1 passage à la certification

Objectifs

- Renforcer ses compétences en pentesting
- Être prêt pour passer la certification eCPPT©

Public visé

- Responsables sécurité
- Auditeurs
- Hackers éthique

Pré-requis

- Expérience en Linux Shell
- Connaissances basiques en Python
- Expérience sur Windows
- Utilisation de Web proxy (Burp ou équivalent)
- Tester Mes Connaissances

Matériels requis

Une machine virtuelle avec Kali Linux installé.

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

Programme de la Préparation à la Certification eCPPT©

Collecte d'Informations & Reconnaissance

- Effectuer la Découverte d'Hôtes et le Scan de Ports sur les Réseaux Cibles
- Énumérer les Informations à partir des Services Fonctionnant sur les Ports Ouverts

Accès Initial

- Effectuer l'Énumération des Noms d'Utilisateurs pour Identifier les Comptes Utilisateurs Valides sur les Systèmes Cibles
- Effectuer des Attaques de Pulvérisation de Mots de Passe pour Identifier les Identifiants Valides pour l'Accès Initial
- Effectuer des Attaques par Force Brute sur les Services d'Accès à Distance pour l'Accès Initial

Test d’Intrusion des Applications Web

- Effectuer l'Énumération des Applications Web pour Identifier les Vulnérabilités Potentielles et les Mauvaises Configurations
- Identifier et Exploiter les Vulnérabilités Communes des Applications Web pour l'Accès Initial (SQLi, XSS, Injection de Commande, etc.)
- Effectuer des Attaques par Brute-Force contre les Formulaires de Connexion
- Exploiter les Composants Vulnérables et Obsolètes des Applications Web
- Exfiltrer les Données et les Identifiants des Applications Web et Bases de Données Compromises

Exploitation & Post-Exploitation

- Identifier et Exploiter les Vulnérabilités ou les Mauvaises Configurations dans les Services
- Identifier et Exploiter les Vulnérabilités d'Escalade de Privilèges
- Extraire et Casser les Hashs de Mots de Passe
- Identifier les Identifiants Non Sécurisés Stockés Localement

Développement d'Exploit

- Développer/Modifier le Code d'Exploit pour l'Accès Initial et la Post-Exploitation
- Identifier et Exploiter les Vulnérabilités de Corruption de Mémoire (Débordement de Pile, Débordement de Tampon)

Test de Pénétration Active Directory

- Effectuer l'Énumération d'Active Directory
- Identifier les Comptes de Domaine avec des Mots de Passe Faibles ou Vides
- Effectuer l'AS-REP Roasting pour Voler les Tickets Kerberos pour l'Authentification
- Effectuer des Techniques de Mouvement Latéral dans Active Directory (Pass-the-Hash, Pass-the-Ticket)
- Obtenir les Privilèges/Accès d'Administrateur de Domaine

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.