+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 Préparation à la certification TCM Security PNPT©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

2 jours (14 heures)

Présentation

La formation TCM Security Practical Network Penetration Tester (PNPT©) vous permettra d'acquérir toutes les ressources nécessaires pour tester la vulnérabilité de vos systèmes, vos applications ou les données de votre entreprise.

À l'aide de cet enseignement, vous deviendrez des experts concernant les tests d'intrusions d'un système ou d'un réseau informatique afin d'y repérer toutes les failles à résoudre.

Grâce à la certification PNPT©, vous pourrez monter en compétences et connaissances dans la cybersécurité pour maîtriser les moyens efficaces pour sécuriser votre système informatique.

Cette formation vous aidera à démontrer toutes les infractions présentes sur vos systèmes dans le but d'y assurer la sécurité dans votre entreprise et d'obtenir un environnement fiable.

Objectifs

- Savoir faire des tests de pénétration
- Comprendre les différentes méthodes d'attaques
- Savoir résoudre la faille d'un système
- Sécuriser un système informatique
- Être prêt pour passer la certification PNPT©

Public visé

- Hackers éthiques

- Pentesteurs
- Auditeurs
- Techniciens SSI
- Chefs de projets

Pré-requis

Avoir une bonne connaissance des réseaux, des systèmes, de la sécurité.

Note : Ambient IT n’est pas propriétaire de PNPT©, cette certification appartient à TCM Security, Inc. ©.

Programme de la formation TCM Security PNPT©

Introduction de l'outil

- Présentation de TCM Security
- Initiation à l'éthique hacking
- Avantages et Inconvénients

Test de pénétration externe

- Analyse et exploitation des vulnérabilités
- Attaquer des portails de connexion (site Web, VPN, O365)
- Collecter des renseignements
  - Sur des informations d'identification violées
  - Sur les médias sociaux
- Contournement de l'authentification multifacteur
- Énumération des tiers pour les fuites de données
- Énumération des services, des ports et des sites Web
- Nom d'utilisateur et énumération de compte

Test de pénétration interne

- Attaques pivotantes
- Attaques de l'homme du milieu (relais SMB, relais LDAP, relais IPv6)
- Attaques par mot de passe et pass-the-hash
- Attaques Kerberoasting
- Analyse des vulnérabilités et énumération des services
- Craquage de hachage

Ingénierie sociale

- Attaques par SMS (smshing)

- Attaques ciblées très médiatisées
- Effectuer de l'hameçonnage par e-mail
- Attaques par téléphone (vishing)
- Attaques ciblées (spearphishing)

Test d'applications Web

- Tests d'injection automatisés et manuels (XSS, SQL)
- Test de parcours de répertoire
- Autres tests manuels en fonction de la langue et du contenu du site
- Téléchargements de fichiers malveillants et exécution de code à distance
- Attaques par mot de passe et contournements d'authentification
- Attaques de session
- Cartographie du site Web
- Analyse et exploitation des vulnérabilités

Essais de pénétration physique

- Reconnaissance et collecte d'informations
- Contournement d'un capteur
- Crochetage
- Imitation
- Clonage de badges
- Piggy backing

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.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2024. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg