Réf : ET_SEC_LP1

Lead Pentester

Encadrer un test d'intrusion ½

Objectif

Les tests d'intrusion sont devenus incontournables dans le domaine de la Cybersécurité. L'objectif de ce cours est de vous transmettre les connaissances méthodologiques et techniques indispensables pour mener et piloter un test d'intrusion et ainsi devenir un bon pentester. Des notions de cadrage et de suivi d'un test d'intrusion vous permettront de cibler le besoin d'un client.

Public	Prérequis	Durée estimée pour le suivi des modules indispensables
Informaticiens	Des connaissances en systèmes et réseaux sont indispensables pour bien appréhender ce cours.	Durée des vidéos : 6h55 Durée des TP : 11h15

Contenu pédagogique

Les modules indispensables

Présentation du cours

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h02.

- Présentation du cours

Le contexte actuel

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h40.

- Définition d'un Lead Pentester et statistiques récentes
- Terminologie
- Principes de la sécurité de l'information
- Définition d'un test d'intrusion
- Les différentes phases d'une attaque
- Aspects réglementaires liés à un test d'intrusion
- Méthodes et framework pour un test d'intrusion

Cadrage et objectifs

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h36.

- Identification des objectifs
- Définition du périmètre
- Démonstration - Framework de pentest ESD Academy
- Enoncé du TP - Questionnaire de pré-engagement
- Gestion et affectation des ressources
- Suivi des objectifs du test
- Règles de pré-engagement (RoE)
- Enoncé du TP - Rédaction d'un contrat de pré-engagement

Préparer son test d'intrusion

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h25.

- Préparation d'une machine pour test d'intrusion
- Automatisation et scripting
- Outils connus
- Démonstration - Rubber Ducky
- Templating de documents
- Démonstration - Suivi du test d'intrusion

Collecte d'informations

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h28.

- Ingénierie des sources publiques (OSINT)
- Relevé passif et actif d'informations publiques
- Démonstration - Présentation des outils OSINT
- Enoncé du TP - Collecte d'informations publiques

Enumération de l'infrastructure

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 1h17.

- Énumération du périmètre - partie 1
- Énumération du périmètre - partie 2
- Techniques d'évasion de pare-feu et IDS
- Enumération des protocoles - partie 1
- Enumération des protocoles - partie 2
- Démonstration - Présentation des outils d'énumération
- Enoncé du TP - Enumération de l'infrastructure

Analyse des vulnérabilités

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h39.

- Scan de vulnérabilités
- Présentation des différents outils
- Démonstration - Présentation d'OpenVAS
- Vulnérabilités connues
- Enoncé du TP - Identification des vulnérabilités

Exploitation

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h57.

- Recherche d'exploits
- Présentation des outils et frameworks d'attaque
- Démonstration - Présentation de Metasploit
- Déploiement et exécution de charges
- Enoncé du TP - Exploitation des vulnérabilités
- Écoute passive et active des infrastructures - partie 1
- Écoute passive et active des infrastructures - partie 2
- Enoncé du TP - Exploitation et analyse des données interceptées
- Bruteforcing

Post exploitation

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 1h52.

- Désactivation des éléments de traçabilité
- Elévation de privilèges - partie 1
- Elévation de privilèges - partie 2
- Démonstration - Présentation des méthodes d'élévation de privilèges
- Etude des persistances
- Mouvements latéraux
- Nettoyage des traces
- Enoncé du TP - Post-exploitation