Pentest 101 : bases du piratage éthique en sécurité

Durée: 1 jour
Public cible: Professionnel TI

À qui s'adresse cette formation ?

- Analystes de sécurité
- Testeurs d'intrusion débutants
- Administrateurs systèmes
- Professionnels TI cherchant une première expérience en piratage éthique

Objectifs de la formation

- Comprendre les bases du test d'intrusion et du piratage éthique
- Découvrir les outils et cadres principaux utilisés en pentest
- Pratiquer l'identification et l'exploitation de vulnérabilités en environnement contrôlé
- Développer des compétences de base en communication des résultats

Description sommaire

Cette formation introductive fournit aux participantes et participants les principes essentiels du test d'intrusion, en combinant compréhension conceptuelle et exercices pratiques. Les apprenantes et apprenants se familiariseront avec les outils, les méthodologies et les pratiques de rédaction de rapports, constituant ainsi une base solide pour aller vers des formations plus avancées en piratage éthique.

Contenu du plan de cours

Module 1 : Introduction au piratage éthique et aux tests d'intrusion

- Définitions, portée et éthique du pentest
- Environnement légal et réglementaire
- Survol des vecteurs d'attaque courants

Module 2 : Méthodologies et cadres de référence

- Reconnaissance et collecte d'information
- Analyse de vulnérabilités et balayage
- Bases de l'exploitation • Post-exploitation et maintien de l'accès

Module 3 : Les outils du métier

- Nmap, Metasploit, Burp Suite, Wireshark
- Atelier pratique : scanner une cible
- Bonnes pratiques pour un environnement de test sécuritaire

Module 4 : Rapport et perspectives

- Structurer un rapport de pentest
- Communiquer les risques aux parties prenantes techniques et non techniques
- Pistes pour certifications et apprentissages futurs

Approche et méthode pédagogique

Exposés structurés permettant de comprendre les concepts fondamentaux du test d’intrusion et du piratage éthique. Démonstrations des outils et des méthodologies utilisés en pentesting pour illustrer les concepts. Exercices pratiques favorisant la manipulation d’outils et l’application concrète des techniques de base. Laboratoires ou environnements contrôlés permettant de s’exercer à l’identification et à l’exploitation de vulnérabilités. Études de cas ou exemples concrets facilitant la compréhension des enjeux réels en cybersécurité. Pratique de rédaction de rapports afin de structurer et communiquer les résultats d’un test d’intrusion.

Prérequis

Connaissances de base en réseaux et systèmes d'exploitation

Recommandations

Familiarité avec l'utilisation en ligne de commande (Linux/Windows) un atout