Fiche du cours

60 h

Titre :

SEC400 - Pentest & Ethical Hacking

Description :

Ce cours forme les étudiants aux bases du test d'intrusion (pentest) et aux méthodes offensives utilisées par les équipes Red Team. Il couvre les principales étapes d'un pentest professionnel : reconnaissance, scanning, exploitation, élévation de privilèges et reporting. Les participants apprennent à utiliser des outils spécialisés, à simuler des attaques réelles dans un cadre légal et à produire des rapports exploitables pour les équipes Blue Team ou sécurité.

Objectifs :

- Comprendre les différentes phases d'un pentest.*
- Utiliser les outils offensifs de base pour détecter et exploiter des failles.*
- Simuler des attaques en environnement contrôlé.*
- Produire des rapports d'analyse clairs et exploitables.

Chapitres :

1. Introduction à l'ethical hacking et au cadre légal*
2. Reconnaissance et collecte d'informations (Nmap, Recon-ng)*
3. Scanning de vulnérabilités et enumeration*
4. Exploitation avec Metasploit et scripts personnalisés*
5. Attaques web et réseau (injections, XSS, brute force, MITM)*
6. Élévation de privilèges et pivoting*
7. Post-exploitation et persistance*
8. Rédaction de rapports techniques et recommandations de mitigation

À la fin :

Vous serez capable de planifier et d'exécuter un test d'intrusion complet dans un environnement encadré, d'identifier et exploiter des vulnérabilités, d'appliquer des techniques d'attaque contrôlées et de formuler des recommandations de sécurité concrètes. Vous disposerez des bases solides pour évoluer vers des rôles Red Team ou poursuivre vers des certifications comme CEH ou OSCP.