Formation Contrer les attaques des hackers et les intrusions

Code : SEC-PENTEST-100 Durée : 5 jours (35 heures)

Public visé

Professionnels de la sécurité informatique, administrateurs système et réseau, consultants en sécurité et/ou toute personne souhaitant débuter dans le domaine du hacking éthique et des tests d'intrusion.

{{< formation-prerequis >}}

Objectifs pédagogiques

À l'issue de cette formation, vous serez capable de :

- Identifier les bases du hacking éthique et les concepts fondamentaux de la sécurité des systèmes d'information
- Déterminer les différentes étapes d'un test de pénétration de base
- Utiliser les principaux outils de reconnaissance et de collecte d'information
- Reconnaître les contre-mesures basiques pour protéger un SI

Programme

Jour 1 - Matin : Introduction et bases du pentesting

- Introduction au hacking éthique et à la cybersécurité
- Cadre juridique et éthique du hacking
- Les phases du test d'intrusion (reconnaissance, scan, exploitation, post-exploitation)

Jour 1 - Après-midi : Outils de collecte

- Google Hacking, Maltego, OSINT

Travaux pratiques indicatifs

- Reconnaissance passive sur cible fictive

Jour 2 - Matin : Reconnaissance active et scan

- Techniques de reconnaissance active
- Scan réseau et ports avec Nmap
- Utilisation avancée de Nmap et scripts NSE

Jour 2 - Après-midi : Scanners de vulnérabilités

- OpenVAS, Nikto pour le Web

Travaux pratiques indicatifs

- Identification et analyse de vulnérabilités

Jour 3 - Matin : Attaques réseau

- Man-in-the-Middle (MITM)
- ARP spoofing, DNS spoofing
- Outil Ettercap

Jour 3 - Après-midi : Contre-mesures réseau

- Sécurisation du réseau local

Travaux pratiques indicatifs

- Exécution d'attaque MITM

Jour 4 - Matin : Exploitation avec Metasploit

- Introduction à Metasploit et payloads
- Création de shellcodes basiques
- Failles basiques

Jour 4 - Après-midi : Travaux pratiques exploitation

- Exploitation de vulnérabilités sur machines virtuelles cibles

Jour 5 - Matin : Post-exploitation

- Collecte d'informations sur la cible
- Techniques de base pour maintenir l'accès
- Backdoors simples

Jour 5 - Après-midi : Documentation et bonnes pratiques

- Élévation de privilèges basique
- Meilleures pratiques et normes
- Tendances cybersécurité

Modalités d'évaluation des acquis

En cours de formation, par des études de cas ou des travaux pratiques. En fin de formation, par un questionnaire d'auto-évaluation.

{{< formation-require >}}

{{< formation-seealso >}}