

GWENDAL LE COGUIC

FORMATIONS

Chaque formation est axée sur des démonstrations pratiques, des exercices interactifs et des discussions sur des situations réelles afin de garantir l'acquisition de compétences clés.

Chaque session peut être suivie :

- sur site ou à distance
- en français ou en anglais
- individuellement ou en groupe

Devis sur demande

Tel: +33 7 69 02 25 10

Email: contact@glc.st

INITIATION AU PENTEST



a. Description

*La formation Pentest est un programme intensif de 3 jours conçu pour initier les **développeurs**, les **administrateurs système** et tous les passionnés de cybersécurité aux fondamentaux du **hacking éthique**. Grâce à une combinaison de **théorie** et d'**exercices pratiques** dans des environnements dédiés, les participants apprendront à **identifier et exploiter les vulnérabilités** des applications web et des services réseaux. Des outils essentiels tels que **Kali Linux**, **Metasploit**, **Burp Suite** et bien d'autres seront abordés. À l'issue de la formation, les participants seront capables de réaliser des audits de sécurité efficaces et de renforcer la protection de leurs infrastructures informatiques.*

b. Objectifs pédagogiques

- Comprendre les fondamentaux du hacking éthique et les limites légales
- Identifier et analyser les vulnérabilités courantes dans les systèmes web et réseaux
- Utiliser des outils standard de l'industrie comme *Kali Linux*, *Metasploit* et *Burp Suite*
- Réaliser des techniques d'exploitation manuelle
- Effectuer des évaluations de vulnérabilité et interpréter les résultats des scans
- Appliquer des méthodologies de *pentesting* pour simuler des attaques réelles

c. Pré-requis

- Connaissances de base en systèmes et réseaux informatiques
- Familiarité avec les systèmes d'exploitation (Linux et Windows)
- Des connaissances de base en programmation ou en scripting sont un plus mais ne sont pas obligatoires

d. Public cible

- Développeurs web
- Administrateurs système
- Ingénieurs Dev(Sec)Ops
- Passionnés de cybersécurité

e. Programme

Jour 1 - Introduction et collecte d'informations

Charte d'audit

- De quoi s'agit-il ?
- Contenu de la charte d'audit

Méthodologie

- Étapes d'une attaque
- Astuces de l'attaquant
- Processus de test

Introduction à Kali Linux

- De quoi s'agit-il ?
- Outils inclus
- Configuration du laboratoire

Collecte d'informations

- Reconnaissance passive et active
- Hacking *Google*, *Shodan*, *GitHub*
- Collecte de données sur les entreprises et les employés
- Technologies
- Enumération ASN
- Enumération, résolution et sondage DNS
- Analyse des ports

Analyse des vulnérabilités

- CWE, CVE et CVSS
- Scanners

Jour 2 - Techniques d'exploitation et sécurité web

Rapport d'audit

- Qu'est-ce que le rapport de test ?
- Contenu du rapport

Tests HTTP

- Exigences de base

- Quoi tester ?
- Extensions de navigateur
- Introduction à *Burp Suite*
- Cross-Site Scripting
- Injection SQL
- Téléchargement de fichiers arbitraires

Autres services réseau

- Shell vs. reverse shell
- Trouver, installer et utiliser des exploits
- Introduction à *Metasploit*
- Exploitation de services : *FTP, SMB, PostgreSQL, WebDAV...*

Jour 3 - Post-exploitation et attaques par mot de passe

Présentation finale

- De quoi s'agit-il ?

Attaques de mot de passe

- Rappel sur la cryptographie : codage, hachage, chiffrement
- Fuites de mots de passe et mots de passe par défaut
- Services en ligne et attaques réseau
- Listes de mots
- Linux vs. Windows

Élévation de privilèges

- Horizontale vs. verticale
- Linux vs. Windows

Post-exploitation

- Persistance
- Éviter les antivirus
- Redirection de ports