Hacking et sécurité : logiciel

Référence : **SECHSL** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Développement Assembleur / C. • TCP/IP.

PROFIL DES STAGIAIRES

• Consultants en sécurité. • Développeurs. • Ingénieurs / Techniciens.

OBJECTIFS

• Comprendre et détecter les faiblesses logicielles d'une application. • Concevoir une architecture logicielle sécurisée.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité offensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

JOUR 1

Introduction à la rétro-conception

- Qu'est-ce que le "cracking" ?
- Les origines
- Pourquoi ?

Les bases

- Le processus
- La pile
- Les registres
- L'assembleur
- Les différents types d'analyse

Analyse statique

- Extraction d'informations statiques
- IDApro
- TP
- Techniques d'obfuscation simples
- Autres outils

Jour 2

Analyse dynamique

- Extraction d'information dynamique
- Immunity debugger
- TP
- Techniques et détections simples
- Autres outils

Les packers/protectors

- Le format PE
- UPX
- TP packer
- Exemple de protector

Jour 3

Les protections avancées

- Téléchargement de DLL
- Mise à plat de graphe d'exécution
- Nanomites
- StolenBytes
- Machines virtuelles

Jour 4

Rétro-conception sous Linux

- Le format ELF
- TP
- Injection de shellcode

Jour 5

Et d'autres langages?

- Java
- Python

TP final