400 FORMATIONS
POUR FAIRE LA DIFFÉRENCE

HACKING ET SÉCURITÉ : LOGICIEL
CODE STAGE : S0004

OBJECTIFS

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

DURÉE

5 jours

PUBLIC

Consultants en sécurité
Développeurs
Ingénieurs / Techniciens

PRÉ-REQUIS

Développement Assembleur / C
TCP/IP

PROGRAMME

Module 1 : JOUR 1

Module 2 : Introduction à la rétro-conception
Qu'est-ce que le « cracking » ?
Les origines
Pourquoi ?

Module 3 : Les bases
Le processus
La pile
Les registres
L'assembleur
Les différents types d'analyse

Module 4 : Analyse statique
Extraction d'informations statiques
IDApro
TP
Techniques d'obfuscation simples
Autres outils

Module 5 : Jour 2

Module 6 : Analyse dynamique
Extraction d'information dynamique
Immunity debugger
TP
Techniques et détections simples
Autres outils

Module 7 : Les packers/protectors
Le format PE
UPX
TP packer
Exemple de protector

Module 8 : Jour 3

Module 9 : Les protections avancées
Téléchargement de DLL
Mise à plat de graphe d'exécution
Nanomites
StolenBytes
Machines virtuelles

Module 10 : Jour 4

Module 11 : Rétro-conception sous Linux
Le format ELF
TP

Injection de shellcode

Module 12 : Jour 5

Module 13 : Et d'autres langages?
Java
Python