Formation failles applicatives
Niveau professionnel

5 jours (possible découpage en 2 x 3 ou 4 jours en approfondissant certains points)

définition et pré-requis

langage assembleur
- les registres
- la memoire
- la pile
- les instructions

Le debugger gdb

Les failles sous linux
- stack overflow
- heap overflow
- return into libc
- format string
- bss overflow

Les shellcode
- les bases
- comprendre les shellcodes
- céer son shellcode

Le debugger Immunity Debbuger

Les failles sous Windows
- stack overflow
- seh

fuzzer
    créer son fuzzer
    utiliser un fuzzer

protection
- le canari
- les implémentations
- les limites de la protection