Ref : DNDAPENTEST2	**Durée :** 5 Jours	**Tarif :** 3 600 €HT

Formation Tests d'intrusion 2

Objectifs de la formation Tests d'intrusion niveau 2:

- Maîtriser les vulnérabilités complexes
- Comprendre le fonctionnement des exploits
- Développer des outils d'attaque
- Contourner les protections système
- Élargir la surface d'attaque

Attention, cette formation ne traite pas des bases des tests d'intrusion ni de l'utilisation de Metasploit, elle va exclusivement au-delà.

Programme de la formation Tests d'intrusions niveau 2:

WEB AVANCE
- Injections SQL en aveugle
- Injections SQL basées sur le temps
- Attaques de désérialisation
- Attaques avancées BDD
- Attaques XXE

ATTAQUES RESEAU
- Scan furtif
- Scapy
- TCP-highjack
- Network Access control (NAC)
  Contourner un portail captif
  Contourner le 802.1X
- VLAN-Hopping
- Rerouter le trafic
  ARP cache poisoning
  DNS spoofing
  Exploitation des protocoles de routing
- Attaque PXE

LES OUTILS DE L'EXPLOITATION AVANCEE
- Python
- Assembleur
- Désassembleurs et debuggers
  GDB/Peda, Radare2

Ollydbg, Immnunity, EDB

LES BASES DU DEVELOPPEMENT D'EXPLOIT

- structure basique d'un exploit (python/perl)
- Win32 shellcoding
- Exploits Metasploit
- Fuzzing
- Sulley/Boofuzz

DEVELOPPEMENT EXPLOITS

- String Format
  - Lire à des adresses
  - Ecrire à des adresses
  - dtor
  - Ecraser la GOT
- Double free
- Off by one
- Integer Overflow

VULNERABILITES APPLICATIVES

- String Format
  - Lire à des adresses
  - Écrire à des adresses
  - dtor
  - Ecraser la GOT
- Double free
- Off by one
- Integer Overflow

BUFFER OVERFLOW

- Stack based
  - Ecraser EIP
  - Sauter vers le shellcode
    - Jump (or call)
    - Pop return
    - Push return
    - Jmp [reg + offset]
    - blind return
    - SEH
    - popadd
    - short jumps et conditionnal jumps
    - stack pivot
  - SEH Exploits
  - Egg Hunting
- Heap based
  - Heap spraying
- Encodage
  - MSFVenom
  - code polymorphique (veniatian encoding)
- Unicode Exploit

CONTOURNEMENT DES PROTECTIONS

- *NX/DEP et ASLR
  - ret2libc
  - retour dans system()
  - ROP
  - écrasement partiel d'EIP

NOP spray
- Stack cookies (canaries)
- SafeSEH
- SEHOP
- Outils divers
Mona
Peda
Pwntools

WIFI
- WEP
- WPA/WPA2
- WPS

PHISHING
- Pieces jointes vérolées
SCRIPT
DDE
- Créer une porte dérobée dans un exécutable
Utiliser les code cave
- Échapper aux antivirus
Assurer la persistance
Le Command & Control

Public

Pentesters expérimentés , Développeurs expérimentés

Pré-requis

Avoir suivi la formation Tests d'intrusion niveau 1 ou posséder une bonne expérience des tests d'intrusion.

Méthodes pédagogiques

Cours magistral avec travaux pratiques et échanges interactifs. Les concepts essentiels développés dans la formation sont illustrés au travers de mises en pratique sur PC permettant d'acquérir des compétences concrètes applicables en tests d'intrusions. Un réseau vulnérable fidèle à la réalité sert de plateforme pour les tests. Tous les outils utilisés sont issus du monde libre et peuvent être réutilisés lors des missions. Les techniques et outils classiques ainsi que modernes sont utilisés tout au long de la formation.