

Programme de formation

Tests d'intrusion et développement d'exploits

But de la formation

- 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.

Pré-requis

- Avoir suivi "Test d'intrusion" ou posséder une bonne expérience des tests d'intrusion.

Type de public

- Pentesters expérimentés,
- Développeurs expérimentés.

Moyens pédagogiques

- Support de cours en Français imprimé
- Cahier d'exercices
- Cahier de corrections
- Ordinateur portable prêté pour la réalisation des exercices

Sanction de la formation

- A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification par HS2.
- Formation délivrée [en partenariat avec HS2](#)

G-echo

6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr



www.g-echo.fr

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

Durée

40 heures (6 jours).

Programme

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, Immunity, 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
 - Ecrire 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 conditional
 - 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

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