

# **HACKING ET SÉCURITÉ : EXPERT**

## **CODE STAGE : S0003**

### **OBJECTIFS**

Acquérir un niveau d'expertise élevé dans le domaine de la sécurité en réalisant différents scénarios complexes d'attaques

En déduire des solutions de sécurité avancées

### **DURÉE**

5 jours

### **PUBLIC**

Administrateurs systèmes / réseaux

Consultants en sécurité

Développeurs

Ingénieurs / Techniciens

### **PRÉ-REQUIS**

Avoir suivi le cours S0002 Hacking Sécurité : Avancé ou posséder les connaissances et compétences équivalentes

Connaissance fondamentale des protocoles réseau (TCP/IP, routage)

Développement occasionnel dans au moins un langage de programmation: Python, PHP, C

Être à l'aise dans l'utilisation des outils classiques du pentest (Kali)

Maîtrise de l'administration Linux (shell) et Windows

Maîtrise des technologies de virtualisation (VirtualBox)

### **PROGRAMME**

Module 1 : JOURS 1 et 2

Techniques de scan : Différents types de scans ; Personnalisation des flags ; Packet-trace ; Utilisation des NSE Scripts

Détection de filtrage : Messages d'erreur / Traceroute ; Sorties nmap ; Firewalking avec le NSE Firewall

Plan d'infrastructure : Problématiques / Erreurs à ne pas faire ; Eléments de défense ; Sécurité physique

Forger les paquets : Commandes de base ; Lire des paquets à partir d'un pcap  
Sniffer les paquets : Exporter au format pcap ; Exporter au format PDF ; Filtrage des paquets avec le filtre filter ; Modifier des paquets via scapy ; Les outils de fuzzing de scapy  
Détournement de communication  
Layer 2 vlan (Trunk, vlan hopping)

## Module 2 : Réseau

Techniques de scan : Différents types de scans ; Personnalisation des flags ; Packet-trace ; Utilisation des NSE Scripts

Détection de filtrage : Messages d'erreur / Traceroute ; Sorties nmap ; Firewalking avec le NSE Firewalk

Plan d'infrastructure : Problématiques / Erreurs à ne pas faire ; Eléments de défense

Forger les paquets : Commandes de base ; Lire des paquets à partir d'un pcap ; Créer et envoyer des paquets

Sniffer les paquets : Exporter au format pcap ; Exporter au format PDF ; Filtrage des paquets avec le filtre filter ; Modifier des paquets via scapy ; Les outils de fuzzing de scapy ; Création d'outils utilisant scapy

Détournement de communications

## Module 3 : Jour 2 (suite)

Découverte de l'infrastructure et des technologies associées

Recherche des vulnérabilités : Côté serveur (recherche d'identifiant, vecteur d'injection, SQL injection) ; Injection de fichiers ; Problématique des sessions ; Web Service ; Ajax ; Côté client (Clickjacking, Xss, XSRF, Flash, Java)

## Module 4 : Système

Metasploit

Attaques d'un service à distance

Attaque d'un client et bypass d'antivirus : Attaque visant Internet Explorer, Firefox ; Attaque visant la suite Microsoft Office ; Génération de binaire Meterpreter ; Bypass AV (killav.rb, chiffrement, padding etc.)

Utilisation du Meterpreter : Utilisation du cmd/Escalade de privilège ; MultiCMD, attaque 5 sessions et plus ; Manipulation du filesystem ; Sniffing / Pivoting / Port Forwarding

Attaque d'un réseau Microsoft : Architecture / PassTheHash ; Vol de token (impersonate token)  
Rootkit

Module 5 : JOUR 3

Module 6 : Web

Découverte de l'infrastructure et des technologies associées

Recherche des vulnérabilités : Côté serveur (recherche d'identifiant, vecteur d'injection, SQL injection) ; Injection de fichiers ; Problématique des sessions ; Web Service ; Côté client (Clickjacking, XSS, CSRF)

Module 7 : JOUR 4

Module 8 : Applicatif

Shellcoding Linux : Du C à l'assembleur ; Suppression des NULL bytes ; Exécution d'un shell

Buffer Overflow avancés sous Linux : Présentation des méthodes standards (Ecrasement de variables ; Contrôler EIP ; Exécuter un shellcode) ; Présentation du ROP et des techniques de bypass des dernières protections (ASLR / NX/ PIE / RELRO)

Module 9 : JOUR 5

Module 10 : TP final

Mise en pratique des connaissances acquises durant la semaine sur un TP final

