

# Cybersécurité : Niveau Expert

Pratiquez les attaques avancées pour mieux se défendre



5 jours



4 - 8 personnes



Valence

## Présentation

Avec des attaques de plus en plus fréquentes et impactantes, les DSI des entreprises doivent savoir les anticiper et mieux se protéger des intrusions sur leurs réseaux. Cette formation met l'accent sur la compréhension technique et la mise en pratique des différentes formes d'attaques existantes. L'objectif est de vous fournir les compétences techniques nécessaires à la réalisation d'audits de sécurité (tests de pénétration), en jugeant par vous-même de la criticité et de l'impact réel des vulnérabilités découvertes sur le SI. La présentation des techniques d'attaques est accompagnée de procédures de sécurité applicables sous différentes architectures (Windows et Linux).



## Objectifs

- Comprendre et détecter les attaques sur un SI
- Définir l'impact et la portée d'une vulnérabilité
- Réaliser un test de pénétration
- Sécuriser un réseau et intégrer des outils de sécurité adéquats

## Public

RSSI, DSI, Consultants en sécurité, Techniciens, Administrateurs systèmes / réseaux, Développeurs

**Prérequis** : Connaissances de l'administration de postes Windows ou Linux, Connaissance de TCP/IP, Utilisation de Linux en ligne de commande

## LES PLUS

- ✓ 70% du temps de la formation consacré aux ateliers pratiques
- ✓ Mise en situation des différentes formes d'attaques existantes
- ✓ Applicabilité directe des outils sous Windows ou Linux
- ✓ Retours d'expériences d'experts de la sécurité informatique

# LE PROGRAMME

## JOUR 1

### Introduction

- Rappel TCP / IP / Réseau Matériel
- Protos / OSI / Adressage IP

### Introduction à la veille

- Vocabulaire et Informations générales
- BDD de Vulnérabilités et Exploits

### Prise d'information

- Informations publiques et Moteur de recherche
- Prise d'information active

### Scan et prise des empreintes

- Énumération des machines
- Scan de ports
- Prise d'empreintes du système d'exploitation
- Prise d'empreintes des services

## JOUR 2

### Attaques réseau

- Idle Host Scanning
- Sniffing réseau, Spoofing réseau
- Hijacking, Déni de service
- Attaques de protocoles sécurisés

### Attaques systèmes

- Scanner de vulnérabilités
- Exploitation d'un service vulnérable distant
- Élévation de privilèges
- Espionnage du système
- Attaques via un malware
  - Génération d'un malware avec Metasploit
  - Encodage de payloads
- Méthodes de détection

## JOUR 3

### Attaques Web

- Cartographie du site et identification des fuites d'informations
- Failles PHP (include, fopen, Upload, etc.)
- Injections SQL
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Bonnes pratiques

## JOUR 4

### Attaques applicatives

- Escape Shell
- Buffer overflow sous Linux
  - L'architecture Intel x86
  - Les registres
  - La pile et son fonctionnement
- Les méthodes d'attaques standards

## JOUR 5

### Challenge final

- Mise en place des connaissances acquises



**CONTACT**

**Elodie Ferrier**

Conseillère formation  
Tél : 04 75 75 87 72  
e.ferrier@drome.cci.fr

**CCI Formation**



En partenariat avec

www.esynov.fr