

## Sécurité Informatique et Réseau les bases, initiation

Référence : SSOM

Niveau : Débutant

Durée : 3 jours (21h.)

Tarif: Nous contacter

Date: 16 Jul 2019

Contact: +225 22469017 / 74622582

### Objectifs

Cette formation est une introduction aux pratiques et aux méthodologies utilisées par les hackers pour s'introduire dans les réseaux d'entreprises. Par un apprentissage technique et une mise en pratique des différentes formes d'attaques existantes, vous acquerez les compétences nécessaires à la réalisation d'audits de sécurité (test de pénétration). Vous apprendrez à évaluer par vous-même la criticité et l'impact des vulnérabilités découvertes sur votre système d'information. La présentation des techniques d'attaques est accompagnée de procédures de sécurité applicables sous différentes architectures (Windows et Linux). Concrètement à l'issue de ce cours vous serez capable de :

- Comprendre et détecter les attaques sur un SI
- Exploiter et définir l'impact et la portée d'une vulnérabilité
- Corriger les vulnérabilités
- Sécuriser un réseau et intégrer les outils de sécurité de base

A l'issue de cette formation, vous pourrez développer vos compétences en suivant un cours Sécurité Informatique et Réseau avancée, perfectionnement (SSSL).

### Public

Cette formation Sécurité du système d'information s'adresse aux RSSI, Consultants en sécurité, Ingénieurs / Techniciens, Administrateurs systèmes / réseaux, ainsi qu'aux personnes en charge de la sécurité informatique.

### Pré-requis

Des connaissances Windows sont importantes pour suivre ce stage dans de bonnes conditions.

### Contenu du cours

#### Introduction

Définitions

Objectifs

Vocabulaire

Méthodologie de test

## Prise d'information

Objectifs

Prise d'information passive (WHOIS, réseaux sociaux, Google Hacking, Shodan, etc.)

Prise d'information active (traceroute, social engineering, etc.)

Bases de vulnérabilités et d'exploits

## Réseau

Rappels modèles OSI et TCP/IP

Vocabulaire

Protocoles ARP, IP, TCP et UDP

NAT

Scan de ports

Sniffing

ARP Cache Poisoning

DoS / DDoS

## Attaques locales

Cassage de mots de passe

Elévation de privilèges

Attaque du GRUB

## Ingénierie sociale

Utilisation de faiblesses humaines afin de récupérer des informations sensibles et/ou compromettre des systèmes

Phishing

Outils de contrôle à distance

## Attaques à distance

Introduction à Metasploit Framework

Scanner de vulnérabilités

Attaques d'un poste client

Attaque d'un serveur

Introduction aux vulnérabilités Web

## Se sécuriser

Les mises à jour

Configurations par défaut et bonnes pratiques

Introduction à la cryptographie  
Présentation de la stéganographie  
Anonymat (TOR)

## Travaux pratiques

Les exercices pratiques représentent 70% du temps de la formation