Formation Cybersécurité : Les fondamentaux

Connaître les différents types d'attaque système pour mieux se protéger

3 jours / 21 heures | **Valence** | **Ref : SECU1**

PRÉSENTATION

Cette formation est une première approche des pratiques et des méthodologies utilisées dans le cadre d'intrusions sur des réseaux d'entreprises. Nous mettons l'accent sur la compréhension technique et la mise en pratique des différentes formes d'attaques existantes. Il s'agit d'une bonne introduction pour toute personne souhaitant acquérir les connaissances techniques de base. La présentation des techniques d'attaques est accompagnée de procédures de sécurité applicables sous différentes architectures (Windows et Linux).

OBJECTIFS DE LA FORMATION

L'objectif est de vous fournir les compétences techniques de base, nécessaires à la réalisation d'audits de sécurité (test de pénétration), en jugeant par vous-même de la criticité et de l'impact réel des vulnérabilités découvertes sur le SI.

—TEST D'INTRUSION

—CYBERSÉCURITÉ

—HACKING

COMPRENDRE la logique d'une intrusion frauduleuse sur un système distant
CONNAÎTRE les mécanismes en jeu dans le cas d'une attaque système
ACQUÉRIR les compétences nécessaires à la mise en place d'un dispositif global garantissant la sécurité des systèmes

PUBLIC VISÉ

Responsables informatique, Techniciens
Administrateurs systèmes / réseaux
Personnels ayant besoin d'acquérir de nouvelles connaissances en sécurité

PRÉREQUIS

Connaissances de base de Windows et de Linux

POUR ALLER PLUS LOIN..

Cybersécurité : Niveau avancé [Ref : SECU2]
Cybersécurité : Niveau expert [Ref : SECU3]
Cloud Computing : Les fondamentaux [Ref : CLOUD1]

LES + DE LA FORMATION

PRATIQUE
70% du temps de formation est consacré aux ateliers pratiques

MISE EN SITUATION
des différentes formes d'attaques existantes

APPLICABILITÉ
directe des outils sous architectures Windows et Linux

Programme

JOUR 1

Introduction sur les réseaux

- Prise d'informations à distance sur les réseaux d'entreprise et les systèmes distants
- Informations publiques
- Localiser le système cible
- Énumération des services actifs

Attaques à distance

- Intrusion à distance des postes clients par exploitation des vulnérabilités sur les services distants et prise de contrôle des postes utilisateurs par troyen

JOUR 2

Attaques à distance

- Authentification par force brute
- Recherche et exploitation de vulnérabilités
- Prise de contrôle à distance

Attaques système

- Attaques du système pour outrepasser l'authentification et/ou surveiller l'utilisateur suite à une intrusion
- Attaque du Bios
- Attaque en local

JOUR 3

Attaques système

- Cracking de mot de passe
- Espionnage du système

Sécuriser le système

- Outils de base permettant d'assurer le minimum de sécurité à son SI
- Cryptographie
- Chiffrement des données
- Détection d'activités anormales
- Initiation à la base de registre
- Firewalling
- Anonymat