Best

Hacking et Sécurité - Les fondamentaux

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

4,4/5 (19 avis)

A distance

28 h

Prix inter : 2.990,00 € HT
Forfait intra : 8.850,00 € HT

Réf.: SE100

L'origine du hacking remonte au milieu des années 50 quand les premiers ordinateurs disponibles dans les universités américaines sont rapidement devenus la proie de d'étudiants avides de "bidouiller" pour s'approprier le système. Ainsi sont nés les hackers qui, profitant de l'avènement d'Internet des décennies plus tard, n'ont cessé de prendre pour cible des systèmes informatiques de plus en plus perfectionnés, allant même jusqu'à pirater des systèmes gouvernementaux. Pour faire face à ces menaces sans cesse croissantes, les DSI attendent des ingénieurs et techniciens qu'ils soient à même de protéger efficacement les systèmes informatiques de leurs organisations. L'objet de cette formation est précisément de leur fournir les compétences et connaissances qui leur permettront de mener à bien cette mission.

A qui s'adresse cette formation ?

Pour qui

- Consultants en sécurité
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux
- Toute personne intéressée par la pratique de la sécurité

Prérequis

- Connaissances de base de Windows ou Linux
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Introduction sur les réseaux

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

2 - 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
- Authentification par brute force
- Recherche et exploitation de vulnérabilités
- Prise de contrôle à distance

3 - Attaques systèmes

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

- Attaque en local
- Cracking de mot de passe
- Espionnage du système

4 - Sécuriser le système

- Outils de base permettant d'assurer le minimum de sécurité à son S.I.
- Cryptographie
- Chiffrement des données
- Détection d'activité anormale
- Initiation à la base de registre
- Firewalling
- Anonymat

Les objectifs de la formation

- Comprendre comment il est possible de s'introduire frauduleusement sur un système distant
- Savoir quels sont les mécanismes en jeu dans le cas d'attaques système
- Acquérir les compétences nécessaires pour mettre en place un dispositif global garantissant la sécurité des systèmes

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une formation très pratique : 70% du temps de la formation est consacré aux ateliers pratiques.
- Un accent particulier est mis sur la pratique des différentes formes d'attaques existantes.
- Chaque présentation technique s'accompagne de procédures de sécurité applicables sous différentes architectures (Windows et Linux).
- Les retours d'expériences de professionnels de la sécurité.
- 88% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Dates 2025 - Référence SE100

Dernières places disponibles Session garantie

du 15 déc. au 18 déc.