

Sécurité système et réseau : Les fondamentaux - 4 jours formation 468

- Vous apprendrez à**
- Analyser les menaces pour la sécurité et protéger les systèmes/données de votre entreprise
 - Diminuer les risques d'attaques grâce à la mise en place de firewalls et au chiffrement de données
 - Évaluer les méthodes alternatives d'authentification des hôtes et des utilisateurs
 - Gérer les risques internes ou connus de l'utilisation d'Internet dans votre entreprise
 - Protéger les utilisateurs de réseaux contre les virus et les applications contaminées
 - Identifier les risques de sécurité menaçant votre entreprise

Objectif Dans un environnement toujours plus dépendant d'Internet, il est indispensable pour les entreprises d'ouvrir leurs systèmes de communication entre leurs différents sites et réseaux virtuels privés mais également de permettre à leurs utilisateurs mobiles de se connecter. Chaque connexion augmente l'exposition aux clients, aux concurrents et aux hackers, exacerbant ainsi les vulnérabilités face aux attaques. Lors de ce cours, vous apprendrez à analyser les risques qui pèsent sur vos réseaux et les étapes à suivre pour choisir et déployer les contre-mesures appropriées pour diminuer l'exposition de vos réseaux aux menaces.

À qui s'adresse cette formation Tous ceux ayant besoin d'acquérir les compétences fondamentales nécessaires pour développer et mettre en œuvre des mesures de sécurité conçues pour protéger les informations d'entreprise des menaces.

Ateliers Les ateliers vous apportent une expérience pratique de l'analyse de la sécurité système et réseau. Ils comprennent :

- Craquage de mot de passe avec des "rainbow tables"
- Scan des systèmes avec MBSA (Microsoft Baseline Security Analyzer)
- Garantir l'accès aux serveurs approuvés par le biais de certificats numériques
- Éviter les accès réseau non désirés avec un firewall personnel
- Chiffrement et signature des données importantes
- Utilisation d'hôtes distants pour mettre en évidence et rectifier des vulnérabilités de communication

Sécurité système et réseau : Les fondamentaux - 4 jours

formation 468

Création d'une entreprise sécurisée

Les vraies menaces à la sécurité

- Intrus internes et externes
- Observation illicite du trafic sur le réseau
- Cheval de Troie
- Virus
- Mise sur écoute

Une politique de sécurité : les bases de votre protection

- Définition de vos objectifs de sécurité
- Évaluation de vos risques

Chiffrement élémentaire

Chiffrement symétrique

- Algorithmes : DES, AES, RC4 et autres
- Évaluation de la longueur et de la distribution des clés

Chiffrement asymétrique

- Génération de clés
- Chiffrement avec RSA
- PGP et GnuPG
- Évaluation du Web of Trust et de PKI

Assurer l'intégrité des données avec le hachage

- Hachage MD5 et SHA
- Protection des données en transit
- Création de signatures numériques

Vérification de l'identité des utilisateurs

Évaluation des plans de mots de passe statiques traditionnels

- Stratégie pour éviter le vol de mots de passe
- Protection contre les attaques d'ingénierie sociale
- Chiffrement des mots de passe pour minimiser l'impact du "sniffing" de mot de passe

Méthodes d'authentification forte

- Éviter les attaques "man-in-the-middle"
- Éviter de rejouer les mots de passe avec les mots de passe à usage unique et ceux à jetons
- Utilisation des biométriques faisant partie de l'authentification à deux facteurs

Authentification des hôtes

- Défauts des adresses IP
- Problèmes des imitations d'adresses et déploiement de contre-mesures
- Solutions pour les réseaux sans fil

Prévention des intrusions système

Découverte des vulnérabilités du système

- Failles du système d'exploitation
- Problèmes des permissions de fichiers
- Limite de l'accès via la sécurité physique

Chiffrement des fichiers pour la confidentialité

- Chiffrement avec les outils spécifiques aux applications
- Récupération des données chiffrées

Renforcement du système d'exploitation

- Verrouillage des comptes utilisateur
- Sécurisation des permissions administrateur
- Protection contre les virus

Défense contre les intrusions réseau

Scan des vulnérabilités

- Restriction des accès aux services critiques
- Éviter les attaques de type "buffer overflow"

Réduction des attaques de type "Déni de Services"

- Sécurisation du DNS
- Limite de l'impact des attaques communes

Déploiement de firewalls pour contrôler le trafic réseau

- Analyse des défauts des filtres de paquets sans états
- Analyse comparative entre les filtres de paquets avec état et les proxies applicatifs
- Éviter les intrusions grâce aux filtres

Création de firewalls réseau

- Évaluation des caractéristiques des firewalls
- Choix d'une architecture et d'un type personnel de firewall

Assurer la confidentialité du réseau

Menaces provenant du réseau local

- Observation illicite du réseau
- Atténuation des menaces provenant d'hôtes
- Partitionnement pour éviter les pertes de données
- Identification des faiblesses des LAN sans fil

Confidentialité des connexions externes

- Confidentialité grâce au chiffrement
- Sécurisation de la couche liaison avec PPTP et L2TP

- Assurance de l'information middleware avec SSL et TLS
- Déploiement de SSH

Protection des données avec IPsec

- Authentification des sites distants
- Tunneling entre sites
- Échange des clés

Gestion de la sécurité de votre entreprise

- Développement d'un plan de sécurité
- Réponse aux incidents
- Énumération des six étapes critiques