

Évaluer les vulnérabilités : Protéger votre entreprise : Travaux Pratiques - 4 jours

formation 589

- Vous apprendrez à**
- Détecter et gérer, grâce aux scanners, les vulnérabilités qui représentent un risque pour votre entreprise
 - Utiliser de réels codes malicieux et évaluer leurs effets sur vos systèmes
 - Configurer les scanners
 - Analyser les résultats des scans de vulnérabilités
 - Évaluer les conseils et alertes
 - Mettre en œuvre une stratégie de gestion des vulnérabilités
- Objectif** Une bonne connaissance des techniques d'attaques et de l'évaluation des vulnérabilités permet de détecter et de traiter les vulnérabilités avant que vos réseaux ne soient attaqués. Dans ce cours, vous apprendrez à configurer et utiliser les scanners de vulnérabilités pour détecter les faiblesses et sécuriser vos réseaux. Vous acquerrez les connaissances nécessaires pour évaluer les risques pour votre entreprise à partir d'un éventail de vulnérabilités et minimiser votre exposition à des brèches de sécurité.
- À qui s'adresse cette formation** Aux auditeurs sécurité, gestionnaires de firewall/IDS, testeurs de sécurité, gestionnaires réseaux et tous ceux qui sont impliqués dans la sécurisation de leurs systèmes d'entreprise. Une expérience de la sécurité réseau du niveau de la formation 468, "Sécurité système et réseau", est nécessaire. Une expérience pratique de TCP/IP est supposée acquise.
- Travaux pratiques** Les exercices vous permettront d'acquérir une expérience pratique de l'évaluation des vulnérabilités :
- Configuration des scanners
 - Énumération et scan des ports
 - Scan de l'infrastructure, des serveurs et des bureaux
 - Exploitation des navigateurs, des IDS, de SQL et de services de fichiers
 - Création de tests de vulnérabilités personnalisés
 - Enquête et prévention des logiciels espion (spyware)
 - Évaluation des risques
 - Interprétation des rapports de scans
 - Identification des faux positifs et faux négatifs
 - Comparaison des résultats des scanners

Évaluer les vulnérabilités : Protéger votre entreprise : Travaux Pratiques - 4 jours formation 589

Concepts fondamentaux

Introduction

- Définition de vulnérabilité, exploit, menace et risque
- Objectifs des évaluations
- Création d'un rapport de vulnérabilités
- Réalisation d'un premier balayage
- Liste CVE (Common Vulnerabilities and Exposure)

Scans et exploits

- Méthodes de détection des vulnérabilités
- Types de scanners
- Scan des ports et découverte du système d'exploitation
- Lister les cibles afin de tester les fuites d'information
- Types d'exploits : worm, spyware, backdoor, rootkits, déni de service (DoS)
- Déploiement des structures d'exploits

Analyse des exploits et des vulnérabilités

Vulnérabilités de l'infrastructure

- Scan de l'infrastructure
- Détection des faiblesses des commutateurs
- Vulnérabilités dans Ethereal et Wireshark
- Attaques des outils de gestion du réseau

Attaques des analyseurs et des IDS

- Faiblesses des firewalls
- Identifier les attaques de l'IDS Snort
- Corruption de la mémoire et déni de service

Vulnérabilités du serveur

- Scans de serveurs : évaluer les vulnérabilités sur votre réseau
- Téléchargement de scripts nocifs et détournement de la directive "include" PHP
- Repérage d'erreurs de validation d'entrée
- Attaques de type buffer overflow (dépassement de mémoire tampon)
- Injection de SQL
- Cross-site scripting (XSS) et vol de cookie

Vulnérabilités du bureau

- Identification des faiblesses du bureau
- Client buffer overflows

- Chargement silencieux : spyware et adware
- Attaque d'erreurs de conception
- Identification des faiblesses des plug-in pour navigateurs

Configuration des scanners de vulnérabilités et création de rapports

Configuration et opérations des scanners

- Choix des ports et des tests dangereux
- Identification des dépendances
- Éviter les faux négatifs
- Création de tests de vulnérabilité personnalisés
- Ajout de nouveaux balayages avec le logiciel Nessus
- Gestion des faux positifs

Création et interprétation des rapports

- Filtrage et personnalisation des rapports
- Interprétation des rapports complexes
- Comparaison des résultats de différents scanners
- Établir un rapport filtré

Évaluation des risques dans un environnement évolutif

Recherche des informations d'alerte

- Utilisation de la NVD (National Vulnerability Database) pour obtenir des informations sur les vulnérabilités et les correctifs
- Évaluation et étude des alertes et annonces de sécurité
- Déterminer le degré de sévérité d'une vulnérabilité
- Utilisation du système CVSS (Common Vulnerability Scoring System)

Identification des facteurs de risques

- Évaluation de l'impact d'une attaque réussie
- Calcul du degré de vulnérabilité
- Évaluation de l'importance des facteurs de risques majeurs
- Évaluation des risques

Gestion des vulnérabilités

Cycle de gestion des vulnérabilités

- Mise en application d'un processus de vulnérabilités
- Standardisation des scans avec OVAL (Open Vulnerability Assessment Language)
- Gestion de la configuration et des correctifs

Controverses sur les vulnérabilités

- Récompense pour la découverte de vulnérabilités
- Prime sur les hackers
- Marchés du bogue et des exploits