Formation Mettre en oeuvre et administrer la sécurité d'un réseau Windows Server 2003

Windows Server 2003 et la plate-forme système de Microsoft intègrent une panoplie très élaborée d'outils de sécurité. Que ce soit pour valider l'identité des collaborateurs avec les autorités de certification et les cartes à puces, pour protéger le trafic réseau avec le pare-feu ISA Server et la solution standard de chiffrement IPSec ou pour maintenir l'ensemble des ordinateurs à jour des correctifs de sécurité avec SUS

Objectifs

- Appréhender globalement le système d'authentification des utilisateurs du simple logon jusqu'aux smart cards et autorités de certification associées
- Définir et mettre en place des standards de configuration sécurisés pour chaque type de serveurs et pour le poste utilisateur incluant le chiffrement des données locales avec EFS
- Savoir mettre en place une gestion des correctifs de sécurité adaptée et solide avec SUS
- Apprendre à contrôler globalement la sécurité du trafic réseau incluant les accès sans-fil et distants, les échanges locaux et le système de pare-feu

Public concerné

- Responsables exploitation
- Responsables systèmes
- Administrateurs

Pré requis

- Expérience dans l'implémentation d'un environnement Windows 2000 ou Windows Server 2003 Active Directory
- Une expérience des ressources organisationnelles telles que le Web, FTP et les serveurs Exchange, des ressources partagées et services réseaux t

Une formation de 5 jours

Caractéristiques
Tarif : 2250 € HT par personne
Numéro de formateur : 11753687675
Nombre d'heures : 35
Référence : MS296
Contact : Patrick LE GOFF
Telephone : 01.76.60.66.10
Email : contact@kaptive.com

Description des modules

num	Module
1	**Planifier et configurer une stratégie d'autorisation et d'authentification**
Détails	- Vue d'ensemble - Groupes et stratégie de groupes de base dans Windows Server 2003 - Créer des relations d'approbation dans Windows Server 2003 - Planifier, mettre en oeuvre et maintenir une stratégie d'autorisation en utilisant des groupes - Composants d'un modèle d'authentification - Planifier et mettre en oeuvre une stratégie d'authentification
2	**Installer, configurer et gérer des autorités de certification**
Détails	- Vue d'ensemble - Présentation des PKI et des autorités de certification - Installer une autorité de certification - Gérer une autorité de certification - Sauvegarder et restaurer une autorité de certification
3	**Configurer, déployer et gérer des certificats**
Détails	- Vue d'ensemble - Configurer des modèles de certificat - Déployer et révoquer des certificats d'utilisateur et d'ordinateur - Gérer des certificats
4	**Planifier, mettre en oeuvre et dépanner des certificats de carte à puce**
Détails	- Vue d'ensemble - Présentation de l'authentification multi facteurs - Planifier et mettre en oeuvre une infrastructure de carte à puce - Gérer et dépanner une infrastructure de carte à puce - Mettre en oeuvre des cartes à puce
5	**Planifier, mettre en oeuvre et dépanner un système de fichiers de chiffrement**
Détails	- Vue d'ensemble - Présentation de EFS - Mettre en oeuvre EFS dans un environnement Microsoft Windows XP autonome - Planifier et mettre en oeuvre EFS dans un environnement de domaine avec une PKI - Mettre en oeuvre un partage de fichiers EFS - Dépanner EFS
6	**Planifier, configurer et déployer une "Baseline" de serveur membre sécurisée**
Détails	- Vue d'ensemble - Vue d'ensemble de la "Baseline" de serveur membre - Planifier une "Baseline" de serveur membre sécurisée - Configurer des paramètres de sécurité additionnels - Déployer des modèles de sécurité
7	**Planifier, configurer et mettre en oeuvre des "Baselines" sécurisées pour des rôles de serveurs**
Détails	- Vue d'ensemble - Planifier et configurer une "Baseline" sécurisée pour des contrôleurs de domaine - Planifier et configurer une "Baseline" sécurisée pour des serveurs DNS - Planifier et configurer une "Baseline" sécurisée pour des serveurs d'infrastructure - Planifier une "Baseline" sécurisée pour des serveurs de fichier et d'imprimante - Planifier et configurer une "Baseline" sécurisée pour des serveurs IIS
8	**Planifier, configurer, mettre en oeuvre et déployer une "Baseline" d'ordinateur client sécurisée**

Détails
- Vue d'ensemble
- Planifier et mettre en oeuvre une "Baseline" d'ordinateur client sécurisée
- Configurer et déployer une "Baseline" d'ordinateur client
- Planifier et mettre en oeuvre une stratégie de restriction logicielle
- Mettre en oeuvre la sécurité pour les clients mobiles

9 Planifier et mettre en oeuvre des services de mises à jour logicielles

Détails
- Vue d'ensemble
- Présentation des services de mises à jour logicielles et de la gestion de mises à jour
- Planifier une stratégie de gestion de mises à jour
- Mettre en oeuvre une infrastructure SUS
- Installer, configurer et maintenir une infrastructure de gestion de mises à jour

10 Planifier, déployer et dépanner une sécurité de transmission de données

Détails
- Vue d'ensemble
- Méthodes de transmission de données sécurisée
- Présentation de IPSec
- Planifier une sécurité de transmission de données
- Mettre en oeuvre des méthodes de transmission de données sécurisées
- Dépanner des communications IPSec

11 Planifier et mettre en oeuvre une sécurité pour les réseaux sans-fil

Détails
- Vue d'ensemble
- Présentation des réseaux sans-fil sécurisés
- Mettre en oeuvre une authentification 802.1x
- Planifier une stratégie WLAN sécurisée
- Mettre en oeuvre un WLAN sécurisé
- Dépanner des réseaux sans-fil

12 Planifier et mettre en oeuvre une sécurité de périmètre avec une sécurité Internet et Acceleration Server 2000

Détails
- Vue d'ensemble
- Présentation de la sécurité Internet et Acceleration Server 2000
- Installer ISA Server 2000
- Sécuriser un réseau de périmètre avec ISA Server 2000
- Publier des serveurs sur un réseau de périmètre
- Sécuriser des ordinateurs ISA Server
- Mettre en oeuvre une sécurité de réseau de périmètre en utilisant ISA Server 2000

13 Sécuriser un accès à distance

Détails
- Vue d'ensemble
- Présentation des technologies et vulnérabilités d'un accès à distance
- Planifier une stratégie d'accès à distance
- Déployer des composants de contrôle de quarantaine d'accès réseau
- Mettre en oeuvre une solution VPN sécurisée