Descriptif de cours

Mise en oeuvre et administration de la sécurité dans un réseau Microsoft Windows Server 2003

CM 2304

Les différents points abordés au cours de ce stage seront mis en application au travers d'ateliers

durée : 5 jours

Ce cours, dirigé par un instructeur et réparti sur cinq journées, traite des compétences MCSA et MCSE que doivent acquérir les professionnels de la sécurité informatique, et répond tout particulièrement aux besoins de formation des personnes qui préparent l'examen de certification 70-299.

Microsoft® Windows Server™ 2003 est le produit phare sur lequel sont basées les solutions d'infrastructure mais il est également question de contenu orienté client lorsque nécessaire. Ce produit didactique a pour but de fournir les compétences fonctionnelles qui permettent de planifier et d'implémenter la sécurité au sein d'une infrastructure.

Ce cours s'adresse aux professionnels de l'informatique qui souhaitent apprendre comment implémenter la sécurité dans Windows Server 2003 afin d'élargir leurs connaissances en matière de plate-forme. Le cours 2810 servira d'introduction pour sensibiliser les stagiaires aux problèmes liés à la sécurité. Ces derniers seront encouragés à participer au cours 2113 afin d'améliorer leurs compétences en matière de conception de la sécurité.

Calendrier du CM 2304

Avril 2009 :	*nous consulter*
Mai 2009 :	11 au 15 à Aix en Provence 11 au 15 à Lyon
Juin 2009 :	*nous consulter*
Juillet 2009 :	27 au 31 à Aix en Provence 27 au 31 à Lyon
Août 2009 :	*nous consulter*
Septembre 2009 :	*nous consulter*
Octobre 2009 :	*nous consulter*
Novembre 2009 :	*nous consulter*
Décembre 2009 :	*nous consulter*
Janvier 2010 :	*nous consulter*
Février 2010 :	*nous consulter*
Mars 2010 :	*nous consulter*

Profil des stagiaires

Le cours s'adresse aux administrateurs système ou aux ingénieurs système qui ont les compétences et les connaissances de base en matière d'implémentation et de déploiement de solutions Microsoft Windows Server 2003 sécurisées. Ce cours a pour but de fournir des compétences de planification (et non de conception) qui vous permettront par la suite d'être autonome au niveau du processus d'implémentation.

Objectifs

À la fin de ce cours, les stagiaires seront à même d'effectuer les tâches suivantes :

- planifier et configurer une stratégie d'authentification et d'autorisation ;
- installer, configurer et gérer des Autorités de certification ;
- configurer, déployer et gérer des certificats ;
- planifier, implémenter et résoudre les problèmes des certificats de carte à puce ;
- planifier, implémenter et résoudre les problèmes du système de fichiers EFS (Encrypting File System) ;
- planifier, configurer et déployer une base sécurisée de serveurs membres ;
- planifier, configurer et implémenter des bases sécurisées pour les rôles des serveurs ;
- planifier, configurer, implémenter et déployer des bases d'ordinateurs clients ;
- planifier et implémenter les services SUS (Software Update Services) ;
- planifier, déployer et résoudre les problèmes de sécurité de la transmission de données ;
- planifier et implémenter la sécurité sur des réseaux sans fil ;
- planifier et implémenter la sécurité de périmètre à l'aide d'Internet Security and Acceleration Server 2000 ;
- sécuriser l'accès à distance.

Connaissances préalables

Pour suivre ce cours, les stagiaires doivent :

- avoir suivi le cours 2810 ou avoir les connaissances équivalentes ;
- avoir déjà implémenté un environnement Active Directory Windows 2000 ou Windows Server 2003 ; connaître les ressources organisationnelles (telles que le Web, le protocole FTP et les serveurs Exchange) et avoir des notions de base sur les ressources partagées et les services réseau, tels que DHCP, DNS et WINS.

Programme MCP (Microsoft Certified Professional)

Ce cours permet aux stagiaires de se préparer à l'examen MCP (Microsoft Certified Professional) suivant

- Examen 70-299 : Implémentation et administration de la sécurité au sein d'un réseau Microsoft Windows Server 2003

2 agences

NEWPORT Communications
Espace Wagner - bâtiment A1
10, rue lieutenant Parayre
Pôle d'activités d'Aix en Provence
13858 Aix en Provence cedex 3

NEWPORT Communications
Tour Crédit Lyonnais
129, rue servient
69326 Lyon Cedex 03

tel Aix : 04 42 39 46 97
tel Lyon : 04 78 63 79 94
fax : 04 42 24 38 93
mail : formation@newport-com.com
web : http://www.newport-com.com/formations/technique/

Documents de cours et logiciels

Le stagiaire dispose d'un manuel de travail complet et de tous les éléments nécessaires pour suivre ce cours.
Le logiciel suivant est fourni au stagiaire :

- CD du stagiaire
- Copie d'évaluation de Windows Server 2003 (usage à caractère pédagogique uniquement).

Support de cours

Le support de cours est en français.

Plan du cours

Module 1 : Planification et configuration d'une stratégie d'autorisation et d'authentification

Ce module explique comment évaluer l'infrastructure de votre organisation, créer et documenter un plan d'authentification et d'autorisation qui permettra d'atteindre le niveau d'accès approprié pour les différentes entités de sécurité. Il décrit également les relations d'approbation, les niveaux fonctionnels de la forêt et du domaine et les principes de sécurité de base.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- déterminer la structure de groupe nécessaire pour un environnement à plusieurs domaines ou à plusieurs forêts ;
- créer des approbations dans un environnement Microsoft Windows Server 2003 ;
- planifier, implémenter et gérer une stratégie d'autorisation et d'authentification dans une organisation à plusieurs forêts ;
- décrire les composants, outils et protocoles qui prennent en charge l'autorisation et l'authentification ;
- planifier et implémenter une stratégie d'autorisation et d'authentification dans une organisation à plusieurs forêts ;
- décrire les stratégies d'autorisation et d'authentification supplémentaires.

Module 2 : Installation, configuration et gestion des Autorités de certification

Ce module décrit les principes de base des systèmes qui vous permettent de sécuriser les communications. Il décrit les méthodes, telles que l'infrastructure à clé publique, qui vous permettent de communiquer sur les réseaux en toute sécurité.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- décrire une infrastructure à clé publique ;
- décrire les applications et les composants qui sont utilisés dans une infrastructure à clé publique
- installer une Autorité de certification ;
- créer et publier des points de distribution de la liste de révocation de certificats et de l'accès aux informations de l'Autorité ;
- sauvegarder et restaurer une Autorité de certification.

Module 3 : Configuration, déploiement et gestion de certificats

Ce module explique comment s'assurer que les certificats sont émis dans les entités de sécurité appropriées et dans le but recherché. Il décrit notamment comment les utilisateurs finaux peuvent effectuer facilement et rapidement le déploiement de certificats.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- configurer des modèles de certificats dans un environnement PKI Microsoft Windows Server 2003 ;
- déployer, inscrire et révoquer des certificats dans un environnement PKI Windows Server 2003 ;
- décrire les applications et les composants qui sont utilisés dans une infrastructure à clé publique
- exporter, importer et archiver des certificats et des clés dans un environnement PKI Windows Server 2003.

Module 4 : Planification, implémentation et résolution des problèmes de certificats de cartes à puce

Ce module explique comment déployer, gérer et configurer des certificats et des modèles de certificats dans un environnement d'infrastructure à clé publique (PKI).
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- comprendre les concepts et les applications de l'authentification multifactorielle ;
- planifier et implémenter une infrastructure de cartes à puce ;

2 agences

NEWPORT Communications
Espace Wagner - bâtiment A1
10, rue lieutenant Parayre
Pôle d'activités d'Aix en Provence
13858 Aix en Provence cedex 3

NEWPORT Communications
Tour Crédit Lyonnais
129, rue servient
69326 Lyon Cedex 03

tel Aix : 04 42 39 46 97
tel Lyon : 04 78 63 79 94
fax : 04 42 24 38 93
mail : formation@newport-com.com
web : http://www.newport-com.com/formations/technique/

- gérer et dépanner une infrastructure de cartes à puce.

Module 5 : Planification, implémentation et résolution des problèmes du système de fichiers EFS (Encrypting File System)

Ce module décrit comment planifier et implémenter un système de fichiers EFS (Encrypting File System), et résoudre les problèmes qui s'y rattachent.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- décrire le système de fichiers EFS et expliquer son fonctionnement ;
- implémenter le système EFS dans un environnement Microsoft Windows XP autonome ;
- planifier et implémenter le système EFS dans un environnement de domaine qui utilise une infrastructure à clé publique (PKI) ;
- implémenter le partage de fichiers EFS ;
- résoudre les problèmes liés au système EFS.

Module 6 : Planification, configuration et déploiement d'une base sécurisée de serveurs membres

La sécurité d'un réseau dépend de la configuration de la sécurité des serveurs qui le composent. Toute violation de la sécurité d'un seul serveur peut compromettre la sécurité de l'ensemble des ordinateurs du réseau et, par conséquent, la sécurité du réseau lui-même. Dans ce module, les stagiaires apprendront à créer des bases sécurisées pour les serveurs.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- décrire l'importance des bases de sécurité et des bases de serveurs membres ;
- planifier une base sécurisée de serveurs membres ;
- configurer des paramètres de sécurité supplémentaires ;
- déployer des modèles de sécurité.

Module 7 : Planification, configuration et implémentation de bases sécurisées pour les rôles des serveurs

Dans ce module, les stagiaires apprendront à créer des bases sécurisées pour les différents rôles des serveurs.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- planifier et configurer une base sécurisée pour les contrôleurs de domaine ;
- planifier et configurer une base sécurisée pour les serveurs DNS (Domain Name System) ;
- planifier et configurer une base sécurisée pour les serveurs d'infrastructure ;
- planifier une base sécurisée pour les serveurs de fichiers et d'impression ;
- planifier et configurer une base sécurisée pour les serveurs IIS (Internet Information Services).

Module 8 : Planification, configuration, implémentation et déploiement d'une base sécurisée d'ordinateurs clients

Dans ce module, les stagiaires apprendront à créer des bases sécurisées pour les ordinateurs clients.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- planifier une base sécurisée d'ordinateurs clients ;
- configurer et déployer une base d'ordinateurs clients ;
- planifier et implémenter une stratégie de restriction logicielle sur les ordinateurs clients ;
- implémenter la sécurité sur les ordinateurs portables.

Module 9 : Planification et implémentation des services SUS (Software Update Services)

Dans ce module, les stagiaires apprendront à planifier et implémenter des stratégies de gestion des mises à jour sur les ordinateurs.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- décrire la nécessité de la gestion des mises à jour et les outils à leur disposition pour implémenter des stratégies de gestion des mises à jour ;
- planifier une stratégie de gestion des mises à jour ;
- implémenter une infrastructure SUS.

Module 10 : Planification, déploiement et résolution des problèmes liés à la sécurité des transmissions de données

Ce module fournit aux stagiaires les informations nécessaires pour planifier la sécurité des transmissions de données et résoudre les problèmes qui y sont liés.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- décrire les différentes méthodes de sécurisation des transmissions de données ;
- décrire l'objectif et le fonctionnement du protocole IPSec ;
- planifier la sécurité des transmissions de données ;
- implémenter des méthodes sécurisées de transmission de données ;
- résoudre les erreurs de transmission de données.

Module 11 : Planification et implémentation de la sécurité sur des réseaux sans fil

La technologie utilisée sur un réseau sans fil permet à plusieurs périphériques de communiquer au moyen de protocoles réseau standard et d'ondes électromagnétiques (et non de câbles réseau) afin de transporter des signaux sur toute ou une partie de l'acheminement. Ce module décrit comment planifier et implémenter la sécurité des réseaux sans fil.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- décrire les composants et les fonctionnalités d'un réseau WLAN sécurisé et d'une infrastructure sans fil ;
- décrire l'authentification 802.1x et son fonctionnement ;
- planifier une infrastructure WLAN sécurisée ;
- implémenter une infrastructure WLAN sécurisée ;
- résoudre les problèmes liés aux composants et aux erreurs WLAN.

Module 12 : Planification et implémentation de la sécurité de périmètre à l'aide d'Internet Security and Acceleration Server 2000

Dans les organisations actuelles, les réseaux sont très souvent interconnectés : les différents réseaux au sein d'une organisation se connectent les uns aux autres, et les réseaux d'entreprise se connectent à Internet. Bien que cette situation offre de nouvelles opportunités pour l'entreprise, elle peut également susciter des inquiétudes en termes de sécurité, de performance et de facilité d'administration.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- décrire les avantages, les modes et les versions d'ISA Server ;
- installer ISA Server 2000 ;
- sécuriser un sous-réseau filtré avec ISA Server 2000 ;
- publier des serveurs.

Module 13 : Sécurisation de l'accès à distance

L'accès à distance permet aux clients d'accès à distance d'accéder aux réseaux d'entreprise comme s'ils étaient directement connectés à ces derniers. Les clients d'accès à distance se connectent au réseau en utilisant des liaisons de communication à distance. La sécurité d'un réseau est compromise si des utilisateurs distants non autorisés parviennent à accéder à des ressources de l'intranet. Pour que la conception de sécurité de l'accès réseau soit efficace, elle doit valider l'identité des clients qui tentent d'accéder aux ressources réseau de l'organisation et faire en sorte que l'accès à des ressources spécifiques soit correctement restreint.
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- décrire les différentes technologies utilisées pour l'accès à distance et les menaces associées à ce dernier ;
- planifier une stratégie d'accès à distance ;
- implémenter et configurer un serveur de réseau privé virtuel (VPN) ;
- déployer les composants du Contrôle de quarantaine pour l'accès réseau.

Prochaines dates

le lundi 11 mai 2009 à En nos locaux d'Aix en Provence
le lundi 11 mai 2009 à En nos locaux de Lyon
le lundi 27 juillet 2009 à En nos locaux d'Aix en Provence
le lundi 27 juillet 2009 à En nos locaux de Lyon

| pour d'autres dates, nous consulter |

2 agences

NEWPORT Communications
Espace Wagner - bâtiment A1
10, rue lieutenant Parayre
Pôle d'activités d'Aix en Provence
13858 Aix en Provence cedex 3

NEWPORT Communications
Tour Crédit Lyonnais
129, rue servient
69326 Lyon Cedex 03

tel Aix : 04 42 39 46 97
tel Lyon : 04 78 63 79 94
fax : 04 42 24 38 93
mail : formation@newport-com.com
web : http://www.newport-com.com/formations/technique/