Windows 2016, sécuriser son infrastructure

Cours Pratique de 3 jours - 21h
Réf : WSI - Prix 2024 : 2 030CHF HT

Ce stage vous apportera les connaissances nécessaires pour sécuriser votre environnement Windows Server 2016, mettre en œuvre les outils de sécurité qui y sont intégrés. Vous verrez comment sécuriser l'OS, l'Active Directory, créer une architecture PKI, protéger vos données et vos accès réseaux.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Connaître les fonctionnalités clés d'une infrastructure sécurisée

Mettre en place un serveur de certificats

Mettre en œuvre la sécurisation de l'Active Directory

Mettre en œuvre NAP avec contrôles d'accès obligatoires

Mettre en œuvre IPSec sous Windows

LE PROGRAMME

dernière mise à jour : 12/2018

1) La sécurité du système d'exploitation

- Option d'installation minimale et mode Core.
- Le contrôle d'accès dynamique des comptes utilisateur.
- Le firewall avancé de Windows 2016 Server.
- Ouverture de session et authentification Windows : authentification NTLM.
- Mise en œuvre de la gestion des mises à jour (WSUS).
- Évaluer, identifier et gérer la sécurité avec les outils : MSAT, MBSA, MSCM.

Travaux pratiques : Paramétrages et réglages de base pour la sécurisation d'un serveur Windows 2016.

2) Certificats et architecture PKI

- Les bases de PKI.
- Gestion des certificats et des clés privées.
- Le rôle de serveur de certificats.
- L'architecture PKI à 2 niveaux.
- Serveur d'autorité de certification : autorité de certification (AD-CS).

Travaux pratiques : Mise en place d'un serveur de certificats. Administration de base des certificats. Sécurisation des accès Web avec HTTPS.

3) Sécurisation de l'Active Directory

- Principe de base pour la sécurité de l'AD.
- Nouveautés des services de certificats Active Directory (AD CS).
- RODC (Read-Only Domain Controler) : intérêt et mise en œuvre.
- Protection par ACL (liste de contrôle d'accès).

Travaux pratiques : Sécurisation de l'Active Directory. Granularité des mots de passe. Installation et paramétrage d'un RODC.

4) La protection de données

- Rappel sur les fondamentaux de la sécurité NTFS, ReFS.

PARTICIPANTS

Administrateurs et ingénieurs systèmes.

PRÉREQUIS

Bonnes connaissances de TCP/IP, de l'administration de Windows Server 2016 et de l'Active Directory.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Mise en place d'EFS. Limites d'EFS.
- BitLocker : cryptage du disque et stockage de la clé de cryptage.
Travaux pratiques : Mise en place d'EFS. Récupération de données avec un agent.

5) La protection d'accès réseau NAP
- Configurer NAP (Network Access Protection).
- Contrôle des PC internes et externes.
- Configurer la mise en œuvre de NAP pour VPN.
- Les serveurs NPS. Composants d'une Infrastructure RADIUS.
Travaux pratiques : Mise en place de NAP avec contrôles d'accès obligatoires. Limiter l'accès au réseau pour les machines non conformes avec DHCP.

6) VPN et IPSec
- Les VPN : principe du tunneling.
- Sécuriser l'accès au domaine avec IPSec.
Travaux pratiques : Mise en œuvre d'IPSec sous Windows. Paramétrage avancé du firewall. Mise en place d'un serveur RADIUS.

LES DATES

Nous contacter