

Opleiding : Windows 2016, beveiliging van uw infrastructuur

Praktijkcursus - 3d - 21u00 - Ref. WSI

Prijs : 1800 € V.B.

Deze cursus geeft je de kennis die je nodig hebt om je Windows Server 2016 omgeving te beveiligen en de ingebouwde beveiligingstools te implementeren. U zult zien hoe u het OS en Active Directory kunt beveiligen, een PKI-architectuur kunt creëren en uw gegevens en netwerktoegang kunt beschermen.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- ✓ De belangrijkste kenmerken van een veilige infrastructuur begrijpen
- ✓ Een certificaatserver instellen
- ✓ Active Directory beveiliging implementeren
- ✓ NAP implementeren met verplichte toegangscontroles
- ✓ IPSec implementeren op Windows

Doelgroep

Systeembeheerders en ingenieurs.

Voorafgaande vereisten

Goede kennis van TCP/IP, Windows Server 2016 administratie en Active Directory.

Opleidingsprogramma

DEELNEMERS

Systeembeheerders en ingenieurs.

VOORAFGAANDE VEREISTEN

Goede kennis van TCP/IP, Windows Server 2016 administratie en Active Directory.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vak kennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

1 Beveiliging besturingssysteem

- Minimale installatieoptie en Core-modus.
- Dynamische toegangscontrole voor gebruikersaccounts.
- De geavanceerde firewall in Windows 2016 Server.
- Windows aanmelding en verificatie: NTLM verificatie.
- Implementatie van updatebeheer (WSUS).
- Beveiliging beoordelen, identificeren en beheren met tools zoals MSAT, MBSA en MSCM.

Praktisch werk

Basisinstellingen en parameters voor het beveiligen van een Windows 2016-server.

2 Certificaten en PKI-architectuur

- PKI-basisbeginselen.
- Beheer van certificaten en privésleutels.
- De rol van de certificaatserver.
- De PKI-architectuur op 2 niveaus.
- Certificeringsautoriteitsserver: certificeringsautoriteit (AD-CS).

Praktisch werk

Een certificaatserver opzetten. Basis certificaatbeheer. Webtoegang beveiligen met HTTPS.

3 Active Directory beveiligen

- Basisprincipe voor DA-beveiliging.
- Nieuw in Active Directory Certificate Services (AD CS).
- RODC (alleen-lezen domeincontroller): voordelen en implementatie.
- ACL-bescherming (toegangscontrolelijst).

Praktisch werk

Beveiligen van de Active Directory. Wachtwoord granulariteit. Installeren en configureren van een RODC.

4 Gegevensbescherming

- Herinnering aan de basisprincipes van NTFS- en ReFS-beveiliging.
- EFS instellen. EFS-limieten.
- BitLocker: schijfcodering en opslag van de coderingsleutel.

Praktisch werk

Implementatie van EFS. Gegevensherstel met een agent.

5 NAP bescherming tegen netwerktoegang

- NAP (Network Access Protection) configureren.
- Controle van interne en externe pc's.
- De implementatie van NAP voor VPN configureren.
- NPS-servers. RADIUS Infrastructuur componenten.

Praktisch werk

Stel NAP's in met verplichte toegangscontroles. Beperk de netwerktoegang voor machines die niet DHCP-compatibel zijn.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

- De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
- Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
- Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

6 VPN en IPSec

- VPN's: het principe van tunneling.
- Domeintoegang beveiligen met IPSec.

Praktisch werk

IPSec implementeren op Windows. Geavanceerde firewall configuratie. Een RADIUS-server instellen.