Publicatiedatum : 09/02/2024

Opleiding : Aantasten en beveiligen van Active Directory

Praktijkcursus - 4d - 28u00 - Ref. ADK
Prijs : 2460 € V.B.

4,6 / 5

Lors de cette formation, vous verrez quelles méthodologies et techniques sont utilisées par les attaquants, de l'accès anonyme jusqu'à la compromission totale de l'environnement. Vous apprendrez comment sécuriser son Active Directory (AD) et gérer une situation de crise après compromission de tout son réseau.

Pedagogische doelstellingen

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

- De interne mechanismen van Active Directory beschrijven
- Beveiligingsfuncties identificeren
- Een robuuste architectuur ontwerpen
- De belangrijkste aanvallen en exploits van een Active Directory-netwerk begrijpen en implementeren
- Tegenmaatregelen implementeren
- Uw Active Directory opnieuw opbouwen in geval van een compromis

Doelgroep

Windows-beheerders, IT-ondersteunend personeel, CISO's, slotters.

Voorafgaande vereisten

Basiskennis van Windows, Active Directory, netwerken en IT-beveiliging.

Praktische modaliteiten

Leer methodes

Méthode expositive, démonstrative et active. Alternance entre présentation, démonstration et mise en pratique.

Opleidingsprogramma

DEELNEMERS

Windows-beheerders, IT-ondersteunend personeel, CISO's, slotters.

VOORAFGAANDE VEREISTEN

Basiskennis van Windows, Active Directory, netwerken en IT-beveiliging.

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 vakkennis 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 Active Directory beveiligingsprincipes

- Een typische Active Directory architectuur begrijpen.
- Begrijpen hoe een Active Directory gecompromitteerd kan worden.
- De belangrijkste aanvalsvectoren die worden gebruikt om Active Directory te compromitteren.
- Herziening van verificatie/autorisatie.
- Een overzicht van de verschillende protocollen.
- De bijbehorende aanbevelingen en goede praktijken begrijpen.

Begeleid praktisch werk

2 Risico's en aanvallen begrijpen

- Overzicht van IS-risicomanagementmethoden.
- Methodologie voor het compromitteren van een Active Directory (on-premise).
- De verschillende stadia van een aanval begrijpen.
- Simuleer aanvallen en analyseer tegenmaatregelen.
- Kwetsbaarheden in de beveiliging opsporen.
- Overzicht van bijbehorende tools.

Praktisch werk

Implementeren van aanvallen en de belangrijkste exploits van een Active Directory netwerk.

3 De AD-infrastructuur harden

- Ontwerp een uithardingsplan.
- Implementeer de bijbehorende richtlijnen.
- Een infrastructuur auditen.
- Verzamel gebeurtenissen op bedrijfsniveau.
- Implementeer de aanbevolen richtlijnen en nieuwe hardening standaarden (PAM, JIT/JEA, etc.).

Begeleid praktisch werk

De verharding van de AD-infrastructuur implementeren.

4 Een gecompromitteerde Active Directory beheren

- De belangrijkste stappen in het managen van een DBA-incident.
- Crisismanagement en communicatie.
- De reconstructie van het AD.

Praktisch werk

Tegenmaatregelen implementeren.

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.

Data en plaats

KLAS OP AFSTAND
2026 : 2 juni, 7 juli, 15 sep., 24 nov.

PARIS LA DÉFENSE
2026 : 26 mei, 30 juni, 8 sep., 17 nov.