

Opleiding : Active Directory offensieve beveiliging, niveau 2

Praktijkcursus - 4d - 28u00 - Ref. SDC

Prijs : 2410 € V.B.

Cette formation vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de votre Active Directory. A la suite de ces attaques, vous acquerez les compétences nécessaires à la réalisation d'un test d'intrusion Active Directory, la méthodologie et les techniques utilisées lors d'une intrusion.

Pedagogische doelstellingen

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

- ✓ Geavanceerde bedieningstechnieken beheersen in een Active Directory omgeving
- ✓ Complexe configuraties en kwetsbaarheden identificeren en misbruiken
- ✓ Werken aan realistische scenario's in gesimuleerde bedrijfsomgevingen

Doelgroep

Pentesters, systeembeheerders, beveiligingsmanagers en cyberbeveiligingsprofessionals.

Voorafgaande vereisten

Bonne connaissance des environnements Windows et des concepts réseau. Ou connaissances équivalentes à celles apportées par le cours "Sécurité offensive de l'Active Directory, niveau 1" (réf. SDB).

Praktische modaliteiten

Praktisch werk

Expositieve, demonstratieve en actieve methode. Afwisselend presentaties, demonstraties en praktische oefeningen.

Opleidingsprogramma

1 Fundamentele theorieën en eerste aanvalstechnieken

- Eerste aanvalstechnieken.
- Inzicht in beheermechanismen (RPC, SMB, WMI, enz.).

DEELNEMERS

Pentesters, systeembeheerders, beveiligingsmanagers en cyberbeveiligingsprofessionals.

VOORAFGAANDE VEREISTEN

Bonne connaissance des environnements Windows et des concepts réseau. Ou connaissances équivalentes à celles apportées par le cours "Sécurité offensive de l'Active Directory, niveau 1" (réf. SDB).

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.

2 Technieken om beveiligingsapparatuur te omzeilen

- Anti-virus omzeilingstechnieken.
- AMSI omleidingstechnieken.
- EDR-omleidingstechnieken.

3 Azure en het in gevaar brengen van Azure-omgevingen

- Basisconcepten van Azure en integratie met Active Directory.
- Herkenning en compromittechnieken in hybride omgevingen.

4 Active Directory en red-teaming

- Informatie verzamelen voor een Red Team-operatie.
- Verberg je aanvallen.
- Offensieve hulpmiddelen voor het rode team.
- Compromittering van SCCM-apparatuur.

5 Ontwikkeling van offensieve tools

- Inleiding tot de ontwikkeling van offensieve tools in C# voor Windows.
- De belangrijkste C# frameworks en bibliotheken die nuttig zijn voor het ontwikkelen van offensieve tools (.NET, WinAPI, P/Invoke).
- Projecten maken in C# voor de ontwikkeling van offensieve tools.
- Gebruik van debugging tools om tools te maken en te onderhouden.
- Presentatie van de belangrijkste Active Directory services (bijv. DNS, LDAP, Kerberos, etc.).
- Aanvallen tegen het Kerberos protocol in Active Directory.
- Ontwikkeling van tools voor het aanvallen en verdedigen van Active Directory.

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 : 23 juni, 29 sep., 1 dec.

PARIS LA DÉFENSE

2026 : 16 juni, 22 sep., 24 nov.