Publicatiedatum : 20/01/2025

Opleiding : Active Directory offensieve beveiliging, niveau 1

Praktijkcursus - 4d - 28u00 - Ref. SDB
Prijs : 2410 € V.B.

In deze cursus leert u de essentiële technieken om het beveiligingsniveau van uw Active Directory te meten. Na deze aanvallen leer je de vaardigheden die nodig zijn om een Active Directory inbraaktest uit te voeren, de methodologie en technieken die tijdens een inbraak worden gebruikt.

Pedagogische doelstellingen

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

- Inzicht in de architectuur en werkingsprincipes van Active Directory (AD)
- Technieken beheersen voor het aanvallen en analyseren van een AD-omgeving
- Veelvoorkomende kwetsbaarheden identificeren en verhelpen
- Preventieve maatregelen implementeren om AD-infrastructuren te beveiligen

Doelgroep

Pentesters, systeembeheerders, beveiligingsmanagers en cyberbeveiligingsprofessionals.

Voorafgaande vereisten

Goede kennis van Windows-omgevingen en netwerkconcepten.

Praktische modaliteiten

Praktisch werk

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

Opleidingsprogramma

1 Fundamentele theorieën en eerste aanvalstechnieken

- Inzicht in beheermechanismen (RPC, SMB, WMI, enz.).
- Identiteits- en toegangsbeheer (NTLM, Kerberos).

DEELNEMERS

Pentesters, systeembeheerders, beveiligingsmanagers en cyberbeveiligingsprofessionals.

VOORAFGAANDE VEREISTEN

Goede kennis van Windows-omgevingen en netwerkconcepten.

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 Erkenning

- OSINT-technieken en -hulpmiddelen (afbeeldingen, e-mails, identifiers, websites, enz.).
- Herkenning van anonieme toegang en geauthenticeerde toegang.
- Geavanceerde technieken voor netwerkherkenning en -exploitatie.

3 Zijdelingse bewegingen

- ADIDNS, WinRM en JEA-vergiftiging, extractie van LAPS-geheimen, gMSA/sMSA,
- Misbruik van MS-SQL vertrouwenskoppelingen, NTLM relaying, dwingen tot authenticatie.
- Kerberos relay, inter-forest pivots, pivots naar Azure (PHS, PTA, ADFS), pivots vanuit Azure (Intune).

4 Verhoging van privileges

- Lokale verhoging van privileges: toegangstoken en impersonatie, onderzoek naar aardappelkwetsbaarheden.
- Softwarebeperkingen omzeilen (AppLocker, beperkte omgevingen zoals Citrix).
- Verheffen van privileges op het domein: bestuderen en misbruiken van ACL's, geavanceerde exploitatie van Kerberos delegatie, ADCS, misbruik van geprivilegieerde groepen.
- Scannen van openbare kwetsbaarheden, authenticatie replay, kerberoasting, misbruik van controlepaden.

5 Geheime extractie en Active Directory persistentie technieken

- Extractie en manipulatie van kritieke geheimen: LSASS, DPAPI, Kerberoasting.
- Persistentie: ADCS (certificaten), Kerberos tickets (gouden, diamanten, saffieren), DSRM, gouden gMSA, misbruik van AdminSDHolder.
- Skeleton sleutel aanmaken, Kerberos delegatie, GPO vergiftiging.
- Uitbreiding van compromissen: onderzoek naar vertrouwensrelaties tussen domeinen en bossen.
- Misbruik van Kerberos delegatie.

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 : 7 apr., 30 juni, 6 okt., 8 dec.

PARIS LA DÉFENSE
2026 : 31 maa., 23 juni, 29 sep., 1 dec.