Publicatiedatum : 31/01/2024

Opleiding : Inbraaktests, het organiseren van uw audit

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

4,6 / 5

Intrusion testing of Pentesting is een technische procedure die wordt gebruikt om het werkelijke potentieel voor inbraak en vernietiging van een IS-infrastructuur door een hacker te bepalen. Deze cursus behandelt de aanpak en tools om dit type test uit te voeren en het uiteindelijke auditrapport op een professionele manier te schrijven.

Pedagogische doelstellingen

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

- Een methodologie verwerven voor het organiseren van een beveiligingsaudit van het type penetratietest van uw IS
- Een eindrapport schrijven na een inbraaktest
- Veiligheidsaanbevelingen doen

Doelgroep

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders. Pentest-auditors.

Voorafgaande vereisten

Goede kennis van IT-beveiliging (hardware, netwerkarchitecturen, applicatiearchitecturen). Vereiste ervaring.

Praktische modaliteiten

Leer methodes

Na een eerste dag gewijd aan herinneringen en het voorbereiden van de omgeving, worden de volgende dagen gewijd aan het uitvoeren van inbraaktesten in levensechte situaties.

Opleidingsprogramma

DEELNEMERS

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders. Pentest-auditors.

VOORAFGAANDE VEREISTEN

Goede kennis van IT-beveiliging (hardware, netwerkarchitecturen, applicatiearchitecturen). Vereiste ervaring.

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 De bedreigingen

- Ontwikkelingen in IS-beveiliging.
- De huidige staat van IT-beveiliging.
- De hackersmentaliteit en -cultuur.
- Wat zijn de risico's en bedreigingen?

2 Auditmethodologie

- De regelgevende context.
- De voordelen van het uitvoeren van een penetratietest, een Pentest, en de verschillende soorten Pentest.
- Hoe penetratietesten integreren in een algemeen beveiligingsproces.
- Leer hoe u een beveiligingsbeheerbeleid en een iteratieve Pentest definieert.
- Het project organiseren en plannen. Hoe bereid je het archief voor?
- De technische reikwijdte van de audit. Het uitvoeren van de Pentest.

Praktisch werk

Een audit uitvoeren.

3 Pentestgereedschappen

- Welke hulpmiddelen moet je gebruiken? Zijn ze echt essentieel?
- Informatie verzamelen. Toegang verkrijgen.
- Verhogen van privileges. Toegang tot het systeem behouden.
- Scan- en netwerktools.
- Hulpmiddelen voor systeemanalyse en webanalyse.
- Tools om werknemers aan te vallen.
- Welke hulpmiddelen kunnen worden gebruikt om de toegang te behouden?
- Operationele kaders.

Praktisch werk

Omgaan met Pentest gereedschappen. Scantools gebruiken.

4 Verslag schrijven

- Informatie verzamelen.
- Het document voorbereiden en het rapport schrijven.
- Algemene analyse van systeembeveiliging.
- Beschrijf de gevonden kwetsbaarheden.
- Doe veiligheidsaanbevelingen.

Groepsdiscussie

Opstellen van een rapport na een inbraaktest.

5 Praktijkvoorbeelden

- Onderscheppen van slecht beveiligde HTTP- of HTTPS-stromen.
- Inbraaktest op een IP-adres.
- Inbraaktests van client-serverapplicaties: FTP, DNS, SMTP.
- Inbraaktests van webapplicaties (SQL-injectie, XSS, kwetsbaarheid van een PHP-module en een CMS).
- Interne inbraaktests: compromittering via een USB-sleutel met boobytraps en via een kwaadaardige PDF.

Praktisch werk

Deelnemers zullen een bedrijfsnetwerk doorlichten op basis van een real-life scenario.

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, 22 sep.

PARIS LA DÉFENSE
2026 : 2 juni, 22 sep.