Publicatiedatum : 30/07/2024

Opleiding : Cyberbeveiliging, het testen van uw omgevingen

aanvallen, detecteren, verzamelen en analyseren

Praktijkcursus - 3d - 21u00 - Ref. CTE

Prijs : 2100 € V.B.

3,8 / 5

In deze geavanceerde training leert u de essentiële technieken om het beveiligingsniveau van uw informatiesysteem te meten. Naar aanleiding van deze aanvallen leert u hoe u de juiste reactie kunt geven en het beveiligingsniveau van uw netwerk kunt verhogen.

Pedagogische doelstellingen

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

- De technieken begrijpen die hackers gebruiken en in staat zijn om hun aanvallen af te slaan
- Het beveiligingsniveau van uw informatiesysteem meten
- Een penetratietest uitvoeren

Doelgroep

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

Voorafgaande vereisten

Goede kennis van IS-beveiliging, netwerken en systemen (met name Linux).

Opleidingsprogramma

DEELNEMERS

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

VOORAFGAANDE VEREISTEN

Goede kennis van IS-beveiliging, netwerken en systemen (met name Linux).

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 Webaanvallen

- OWASP: organisatie, hoofdstukken, Top10, handleidingen, hulpmiddelen.
- Ontdek de infrastructuur en bijbehorende technologieën, sterke en zwakke punten.
- Clientzijde: clickjacking, CSRF, cookiediefstal, XSS, componenten (Flash, Java). Nieuwe vectoren.
- Serverzijde: authenticatie, sessiediefstal, injecties (SQL, LDAP, bestanden, commando's).
- Opname van lokale en externe bestanden, aanvallen en cryptografische vectoren.
- Omzeilen en omzeilen van bescherming: voorbeeld van WAF-omzeilingstechnieken.
- Burp Suite, ZAP, Sqlmap, BeEF tools.

Rollenspel
Presentatie en kennismaking met omgevingen en gereedschappen. Implementatie van verschillende webaanvallen onder echte omstandigheden aan server- en clientzijde.

2 Indringers detecteren

- Werkingsprincipes en detectiemethoden.
- Marktspelers, overzicht van de betrokken systemen en toepassingen.
- Scanners voor netwerken (Nmap) en toepassingen (webtoepassingen).
- IDS (Intrusion Detection System).
- De voordelen en beperkingen van deze technologieën.
- Hoe moeten ze worden gepositioneerd in de bedrijfsarchitectuur?
- Marktoverzicht, gedetailleerde studie van SNORT.

Rollenspel
Presentatie en kennismaking met omgevingen en hulpmiddelen. Installatie, configuratie en implementatie van SNORT, schrijven van aanvalshandtekeningen.

3 Informatie verzamelen

- De heterogeniteit van bronnen. Wat is een veiligheidsgebeurtenis?
- Informatiebeheer beveiligingsgebeurtenissen (SIEM). Gebeurtenissen verzameld uit de IS.
- Systeemlogs van apparatuur (firewalls, routers, servers, databases, etc.).
- Passief verzamelen in luistermodus en actief verzamelen.

Rollenspel
Loganalyseprocedure. Een adres geolokaliseren. Logs van verschillende bronnen correleren, bekijken, sorteren en zoeken naar regels.

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 : 25 maa., 24 juni, 7 okt., 9 dec.

PARIS LA DÉFENSE
2026 : 24 juni, 7 okt., 9 dec.