Publicatiedatum : 13/05/2024

Opleiding : Forensisch netwerkonderzoek

Praktijkcursus - 3d - 21u00 - Ref. FOF
Prijs : 2100 € V.B.

Deze training stelt je in staat om de kennis te verwerven die nodig is om de sporen te identificeren die worden achtergelaten wanneer er wordt ingebroken op een computersysteem, om onderzoeken uit te voeren op de verschillende soorten netwerken en om op de juiste manier het bewijs te verzamelen dat nodig is voor juridische procedures.

Pedagogische doelstellingen

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

- De kennis verwerven die nodig is om forensische analyses op een netwerk uit te voeren
- Methoden verwerven om bekabelde en draadloze netwerken te onderzoeken
- De methodologie verwerven voor het schrijven van een forensisch auditrapport over penetratietests
- De sporen identificeren die achterblijven wanneer een computernetwerk wordt gekraakt

Doelgroep

Systeem- en netwerkingenieurs/beheerders, beveiligingsmanagers

Voorafgaande vereisten

Goede kennis van IT-beveiliging en netwerken/systemen

Praktische modaliteiten

Praktisch werk

Training waarin theorie en praktijk worden afgewisseld. Alles wat je leert, breng je in de praktijk.

Opleidingsprogramma

DEELNEMERS

Systeem- en netwerkingenieurs/beheerders, beveiligingsmanagers

VOORAFGAANDE VEREISTEN

Goede kennis van IT-beveiliging en netwerken/systemen

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 Moderne cybercriminaliteit

- Soorten misdrijven.
- Beheerskader voor beveiligingsincidenten, CERT.
- Laboratoria opzetten: de hulpmiddelen die nodig zijn om netwerken te onderzoeken.
- Netwerkaanvallen analyseren en begrijpen.
- Netwerkintrusiedetectie.
- Beschermingsmiddelen, Franse wetgeving.

Praktisch werk

Netwerkanalyse van DDOS-aanvallen, infecties en BotNet-verkeer naar C2

2 Digitaal bewijs

- Definitie, rol, types en archiveringsregels.
- Evalueren en beveiligen van de elektronische elementen van een plaats delict.
- Verzamel en behoud de integriteit van elektronisch bewijs.

Praktisch werk

Gegevens bit voor bit dupliceren, integriteit controleren. Netwerkgegevens vastleggen. Analyse van digitale gegevens

3 Forensische netwerkanalyse

- Inzicht in netwerkarchitectuur.
- Netwerkaanvallen en kwetsbaarheden begrijpen.
- Methoden voor het onderzoeken van bedrade en draadloze netwerken.
- Frame-opnames analyseren.
- Verschillende soorten aanvallen identificeren: ARP Storm, DHCP Starvation, ARP Spoofing, netwerkscanning, exfiltratie van gegevens, etc.

Praktisch werk

Voorbeelden van aanvallen op bedrade en draadloze netwerken. Forensisch onderzoek van draadloze verbindingen gedetecteerd op een plaats delict.

4 Controle en beveiliging

- Inbraakdetectie- en preventiesystemen.
- Assimilatie en implementatie van de inbraaktestfasen.
- Veiligheidstoezicht.

Praktisch werk

Analyseren van netwerken en inbraken met behulp van IDS/IPS. Onderzoeken uitvoeren met de Snort tool.

5 Forensische onderzoeksrapporten

- Het belang van onderzoeksrapporten begrijpen.
- Methodologieën en sjablonen voor het schrijven van forensische auditrapporten en penetratietests.

Data en plaats

KLAS OP AFSTAND
2026 : 27 mei, 7 okt.

PARIS LA DÉFENSE
2026 : 27 mei, 7 okt.

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.