Publicatiedatum : 01/07/2024

Opleiding : Forensisch onderzoek Android

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

Deze training geeft je de kennis die je nodig hebt om onderzoeken uit te voeren op de verschillende Android-systemen en 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 Android uit te voeren
- Verzamelen en bewaren van de integriteit van elektronisch bewijsmateriaal
- Analyse na de inbraak

Doelgroep

Systeem- en netwerkingenieurs/beheerders, beveiligingsmanagers.

Voorafgaande vereisten

Goede kennis van IT-beveiliging, netwerken/systemen en Android-systemen.

Praktische modaliteiten

Praktisch werk

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

Opleidingsprogramma

1 Forensische analyse van een mobiel systeem

- Forensisch computeronderzoek.
- Soorten computercriminaliteit op mobiele systemen.
- Rol van de IT-onderzoeker.

DEELNEMERS

Systeem- en netwerkingenieurs/beheerders, beveiligingsmanagers.

VOORAFGAANDE VEREISTEN

Goede kennis van IT-beveiliging, netwerken/systemen en Android-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.

2 Moderne cybercriminaliteit

- Soorten misdrijven.
- Beheerskader voor beveiligingsincidenten, CERT.
- De labs opzetten: tools die nodig zijn om Android te onderzoeken.
- Analyseren en begrijpen van aanvallen op mobiele systemen.
- Beschermingsmiddelen, Franse wetgeving.

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

3 Digitaal bewijs

- Definitie, rol, types en archiveringsregels.
- Evalueren en beveiligen van de elektronische elementen van een plaats delict.
- Verzamelen en bewaren van de integriteit van bewijsmateriaal.

Praktisch werk
Bit-voor-bit duplicatie, integriteit, bestandsherstel en gegevensanalyse.

4 Forensische grondslagen voor mobiele systemen

- Inzicht in de architectuur van mobiele systemen en simkaarten.
- Forensische technieken voor mobiele systemen.
- Forensische processen voor mobiele systemen.

Praktisch werk
Analyse van mobiele toepassingen en malware. Forensisch onderzoek met Santoku-distributie.

5 De basisbeginselen van forensische analyse van Android-systemen

- Studie van Android-modelarchitecturen.
- Studie van softwarecomponenten: Kernel, Android Runtime, Bibliotheken.
- Studie naar de beveiliging van het Android-systeem.

Praktisch werk
Een forensisch Android-onderzoekslab opzetten.

6 Technieken voor het extraheren en analyseren van gegevens uit Android-systemen

- Gegevensextractie en acquisitietechnieken.
- Verzamelen van vluchtige en niet-vluchtige gegevens.
- Android-systemen voor gegevensanalyse en -herstel.
- Analyse en reverse engineering van Android-toepassingen.
- Sluittechnieken omzeilen.
- Verkrijg root-toegangsrechten.
- Technieken voor het extraheren van gegevens uit software van derden.

Praktisch werk
Globaal onderzoek van een vastgelegd beeld van een Android systeem: Omzeilen van encryptie. RAM verzamelen en analyseren. Android rooten en gegevens uit toepassingen van derden halen.

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.

7 **Forensische onderzoeksrapporten**

- Het belang van relaties begrijpen.
- Copywritingmethoden en sjablonen.

Data en plaats

KLAS OP AFSTAND
2026 : 20 mei, 12 okt., 23 nov.

PARIS LA DÉFENSE
2026 : 20 mei, 12 okt., 23 nov.