Forensics Android

Cours Pratique de 3 jours - 21h
Réf : FOL - Prix 2024 : 2 390CHF HT

Cette formation vous permettra d'acquérir les connaissances nécessaires pour effectuer de l'investigation sur les différents systèmes Android et collecter correctement les preuves nécessaires à des poursuites judiciaires.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Acquérir les connaissances pour réaliser les analyses forensics sur Android

Collecter et préserver l'intégrité des preuves électroniques

Analyser l'intrusion a posteriori

TRAVAUX PRATIQUES

Formation alternant théorie et pratique. Tout ce qui est appris sera expérimenté.

LE PROGRAMME

dernière mise à jour : 05/2022

1) L'analyse forensic d'un système mobile

- Informatique judiciaire.
- Les types de crimes informatiques sur les systèmes mobiles.
- Rôle de l'enquêteur informatique.

2) La cybercriminalité moderne

- Types de criminalité.
- Cadre de gestion d'un incident de sécurité, CERT.
- Mise en place des labs : outils nécessaires pour investigation Android.
- Analyser et comprendre les attaques sur les systèmes mobiles.
- Outils de protection, législation française.

Travaux pratiques : Analyse réseaux d'attaques DDOS, d'infection et de traffic BotNet vers C2.

3) La preuve numérique

- Définition, rôle, types et règles de classement.
- Evaluer et sécuriser les éléments électroniques d'une scène de crime.
- Collecter et préserver l'intégrité des preuves.

Travaux pratiques : Duplication bit à bit, intégrité, récupérer des fichiers et analyser des données.

4) Bases de forensic des systèmes mobiles

- Comprendre l'architecture des systèmes mobiles et cartes SIM.
- Techniques de forensic des systèmes mobiles.
- Processus forensic des systèmes mobiles.

Travaux pratiques : Analyse des applications et malwares sous mobile. Investigation forensic avec la distribution Santoku.

5) Les bases de l'analyse forensic des systèmes Android

- Etude des architectures des modèles d'Android.

PARTICIPANTS

Ingénieurs / administrateurs systèmes et réseaux, responsables sécurité.

PRÉREQUIS

Bonnes connaissances en sécurité informatique, en réseaux/systèmes et en systèmes Android.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Etude des composants logiciels : Kernel, Android Runtime, Librairies.
- Etude de la sécurité des systèmes Android.

Travaux pratiques : Mise en place d'un lab d'investigation forensic Android.

6) Techniques d'extraction et analyse des données des systèmes Android

- Techniques d'extraction et acquisition des données.
- Collecte des données volatiles et non volatiles.
- Systèmes d'analyse et recouvrement des données Android.
- Analyse et reverse engineering des applications Android.
- Bypasser les techniques de verrouillage.
- Obtention des droits d'accès root.
- Techniques d'extraction des données des logiciels tiers.

Travaux pratiques : Investigation globale d'une image capturée d'un système Android : Bypass des chiffrements. Collecter, analyser la mémoire vive. Root d'Android et extraction des données des applications tiers.

7) Rapports d'investigation forensic

- Comprendre l'importance des rapports.
- Méthodologies de rédaction et templates.

LES DATES

CLASSE À DISTANCE
2024 : 28 oct.