Forensics réseaux

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

Cette formation vous permettra d'acquérir les connaissances pour identifier les traces laissées lors de l'intrusion d'un système informatique, effectuer de l'investigation sur les différents types de réseaux, 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 un réseau

Acquérir les méthodes d'investigation des réseaux filaires et non filaires

Acquérir la méthodologies de rédaction d'un rapport d'audit forensic des tests d'intrusion

Identifier les traces laissées lors de l'intrusion sur un réseau informatique

TRAVAUX PRATIQUES

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

LE PROGRAMME

dernière mise à jour : 05/2022

1) La cybercriminalité moderne

- Types de criminalité.
- Cadre de gestion d'un incident de sécurité, CERT.
- Mise en place des labs : outils nécessaires pour l'investigation des réseaux.
- Analyser et comprendre les attaques réseaux.
- Détection réseau d'intrusions.
- Outils de protection, législation française.

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

2) 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 électroniques.

Travaux pratiques : Dupliquer les données bit à bit, vérifier l'intégrité. Capture des données du réseau. Analyse des données numériques

3) Analyse forensic des réseaux

- Comprendre l'architecture des réseaux.
- Comprendre les attaques et vulnérabilités des réseaux.
- Méthodes d'investigation des réseaux filaires et non filaires.
- Analyser des captures de trames.
- Identifier différents types d'attaques: ARP Storm, DHCP Starvation, ARP Spoofing, scan réseau, exfiltration de données…

Travaux pratiques : Exemple d'attaques sur les réseaux filaires ou non filaires. Investigation forensic des connexions sans fils détectées sur une scène de crime.

PARTICIPANTS

Ingénieurs/administrateu rs systèmes et réseaux, responsables sécurité

PRÉREQUIS

Bonnes connaissances en sécurité informatique et en réseaux/systèmes

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.

4) Audit et sécurité

- Systèmes de détection et prévention des intrusions.
- Assimilation et réalisation des étapes de tests d'intrusion.
- Supervision de la sécurité.

Travaux pratiques : Analyser les réseaux et intrusions avec des IDS/IPS. Appliquer les investigations en utilisant l'outil Snort.

5) Rapports d'investigation forensic

- Comprendre l'importance des rapports d'investigation.
- Méthodologies de rédaction et templates des rapports d'audit forensic des tests d'intrusion.

LES DATES

CLASSE À DISTANCE
2024 : 16 oct.