| | | |
|---|---|---|
| CNFCPP | **FICHE PROGRAMME D'UNE ACTION DE FORMATION** | Réf: **FORM.FINC.02**<br>Version : 00<br>Date d'application : 20/04/09 |

**Thème : Cybersécurité et Cybercriminalité: Aspects Juridiques, Organisationnels et Techniques**

**Population cible** :

- consultants en sécurité ;
- responsable des Systèmes d'Information ;
- analystes réseau ;
- professionnel de l'IT souhaitant apprendre les concepts vitaux pour mener une investigation inforensique.

| **Objectifs de le formation :** | **Objectifs pédagogiques :** |
|---|---|
| Cet atelier permettra aux participants d'acquérir une réelle connaissance de la cybercriminalité et des compétences en analyse sécurité et inforensique des réseaux et des systèmes. L'atelier abordera naturellement l'analyse des trafics de réseaux, l'amélioration de la sécurité des réseaux et leur fiabilité. Outre ces points, l'atelier se penchera sur la protection des réseaux contre les attaques malicieuses et criminelles. Les participants auront l'opportunité d'aborder les techniques d'identification des modèles de trafics suspects, d'identifier la vulnérabilité d'un hôte dans un réseau ; et les techniques de traitement et de gestion des machines compromises ou infectées.<br><br>En d'autres termes, cet atelier de formation donnera les outils nécessaires aux participants afin de mener à bien des investigations sur des traces réseaux dans un contexte de réponse à incident ou d'inforensique, depuis la collecte des données jusqu'à leur analyse et interprétation. Cette formation s'appuie sur les points importants des systèmes Windows que tout investigateur en inforensique se doit de connaître. | Une connaissance de base de la sécurité des systèmes d'information. |

| **Jours** | **Contenus/ Concepts clés à aborder** | **Méthodes et Moyens Pédagogiques** | **Durée (Heures)** | |
|---|---|---|---|---|
| | | | **Théorie** | **Pratique** |
| **J1** | Accueil, enregistrement et ouverture du séminaire.<br><br>**<u>Cadre de la cybercriminalité</u>**<br>▪ Cadre juridique<br>▪ Cadre institutionnel<br>▪ Cadre technique<br><br>**<u>Fondamentaux de l'inforensique</u>**<br>▪ Objectif de l'inforensique.<br>▪ Présentation des cas d'inforensique les plus communs.<br>▪ Types d'informations stockées | Exposés, travaux pratiques et échanges interactifs. | **3** | **3** |

| | | | | |
|---|---|---|---|---|
| | électroniquement.<br>▪ Localisation des preuves électroniquement stockées<br>▪ Acquisition et analyse des données volatiles.<br>▪ Les systèmes de fichiers : généralités<br>▪ Rapport de preuves et présentations de celles-ci.<br>▪ Méthodologie inforensique.<br>**Acquisition et analyse**<br>▪ Acquisition des preuves : généralités.<br>▪ Conservation des preuves.<br>▪ Méthodes d'acquisition.<br>▪ Kit de survie de l'expert inforensique.<br>▪ Outils et technique d'acquisition d'images disques complètes.<br>▪ Acquisition de données sur le réseau.<br>▪ Les outils inforensique graphiques.<br>▪ Étapes usuelles et outils inforensiques associés.<br>▪ Acquisition des fichiers supprimés | | | |
| J2 | **Inforensique Windows : Analyse des Emails et de la base de registres (1)**<br>▪ Inforensique des Emails.<br>▪ Emails Microsoft Outlook/Outlook Express/Windows.<br>▪ Emails des WebMails.<br>▪ Microsoft Exchange.<br>▪ Lotus Notes.<br>**Inforensique Windows : Analyse des Emails et de la base de registres (2)**<br>▪ Inforensique en profondeur de la base de registres.<br>▪ Authentification.<br>▪ Informations système.<br>▪ Preuves diverses.<br>▪ Historique de recherche sous XP et Win7. | Exposés, travaux pratiques et échanges interactifs. | 3 | 3 |
| J3 | **Inforensique Windows : Analyse des Emails et de la base de registres (3)**<br>▪ Accès aux URLs.<br>▪ Documents récents.<br>▪ Boites de dialogue 'Ouvrir / Sauvegarder / Exécuter. | Exposés, travaux pratiques et échanges interactifs. | 3 | 3 |

| | | | | |
|---|---|---|---|---|
| | ▪ Historique de l'exécution d'application.<br>▪ Éditeur/Création/Version.<br>**<u>Inforensique Windows : Analyse des Emails et de la base de registres</u> (4)**<br>▪ Numéro de série unique.<br>▪ Lettre du dernier disque<br>▪ Nom des volumes.<br>▪ USB.<br>▪ Regripper, d'Harlan Carvey.<br>▪ Registry Viewer, d'Access Data. | | | |
| **J4** | **<u>Inforensique Windows : Analyse des artefactes et fichiers de journalisation</u>**<br>▪ Analyse mémoire, mémoire virtuelle et espace non alloué.<br>▪ Conversations Facebook live, MSN Messenger, Yahoo, AIM, GoogleTalk.<br>▪ URLs d'IE8 InPrivate/Recovery.<br>▪ WebMails de Yahoo, Hotmail, Gmail.<br>▪ Inforensique des fichiers contenant des preuves sensibles.<br>▪ Analyse inforensique des journaux d'évènements de Windows.<br>**<u>Inforensique Windows : Inforensique du navigateur web</u>**<br>▪ Inforensique des navigateurs web.<br>▪ Internet Explorer.<br>▪ Localisation des fichiers clés de l'inforensique FF2 and FF3.<br>▪ Web Historian, de Mandiant.<br>▪ FTK, de FTK.<br>▪ FoxAnalysis. | Exposés, travaux pratiques et échanges interactifs. | 3 | **3** |
| **J5** | **<u>Exercices pratiques</u>**<br>Une mise situation d'analyse inforensique clôturera cet atelier de formation.<br>Ce cas pratique final permettant aux participants d'utiliser l'ensemble des outils et méthodes découverts tout au long de la formation afin de construire un rapport inforensique sur un cas d'étude spécialement | Exposés, travaux pratiques et échanges interactifs. | 2h | **2h** |

| | | | | |
|---|---|---|---|---|
| | mis en place.<br>Evaluation des auditeurs<br>Evaluation du séminaire, remise des attestations et clôture de l'atelier. | | | |
| **Total** | | | **14h** | **14h** |

| **Critères et indicateurs d'évaluation QCM** |
|---|
| |

**NB** : *Fiche à établir par l'opérateur de formation*

**Case réservée à l'administration :**

**Avis technique :** ……

……

……

**Fait à ……. le ……..Signature**