SETC Training Corporate Logo

Formation sécurité informatique: La criminalistique Windows de A à Z (WIFOREFR, 4 jours)

Description

Le cours Formation sécurité informatique : La criminalistique Windows de A à Z explore les complexités de la collecte de preuves numériques sur tout ce qui est Windows. La formation commence par une discussion générale sur les types de preuves et les techniques connexes de collecte de preuves. Elle est suivie d'une exploration détaillée de la réponse à l'amour et de la collecte de données volatiles et non volatiles sur la plate-forme Windows. La formation couvre l'analyse de la mémoire de Windows, des systèmes de fichiers FAT et NAzure DevOps et de divers artefacts Windows, notamment les navigateurs Web, les journaux d'événements, les fichiers de pages, etc.

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Premières étapes

- Le processus de la criminalistique : Concepts et exigences
- Comprendre l'environnement du laboratoire
- Principes généraux : Intégrité, chaîne de contrôle et plus encore
- Phases de l'enquête
- Processus de haut niveau
- Similitudes et différences : Windows 7, Windows 10 et Windows Server
- Obtenir des images du système de fichiers
- Techniques pour obtenir des images de systèmes de fichiers
- Création d'une boîte à outils
- Construction d'un laboratoire
- Créer un modèle de rapport

Réponse en direct : Collecte de données volatiles

- Explorer les exigences de la police scientifique
- Réaction immédiate et triage
- Exploration de Live Response
- Comprendre la différence entre les données volatiles et non volatiles
- Comprendre les stratégies d'intervention locales, distantes et hybrides
- Méthodes réactives et proactives
- Quelles données collecter ?
- Rédaction du rapport

Collecte des données - Informations volatiles

- Aperçu de l'information volatile
- Explorer les outils disponibles
- Collecte des utilisateurs connectés
- Collecte des dossiers ouverts
- Collecte des informations et de l'état du réseau
- Collecte d'informations sur le processus
- Collecte des mappages entre processus et ports
- Collecte de la mémoire des processus
- Exploration des concepts de presse-papiers

Collecte d'informations sur le conducteur de service
Collecte de l'historique des commandes
Collecte des lecteurs mappés
Collecte des actions

Collecte des données - Informations non volatiles

Aperçu des informations non volatiles
Explorer les outils disponibles
Explorer le registre
Effacer le fichier de la page
Désactivation du dernier accès
Gestion des programmes automatiques
Exploration des journaux d'événements
Collecte d'informations sur les appareils et autres informations

Analyse en direct

Analyse des résultats de l'analyse initiale
Obtenir des métadonnées de fichiers
Construire une ligne de temps
Examen de l'historique des commandes de l'utilisateur
Collecte des hachages de fichiers
Dumping RAM
Aller de l'avant

Analyse de la mémoire Windows

A propos de l'architecture mémoire - Concepts essentiels
Exploration de la collecte et des vidages de mémoire
Exploration des méthodes de vidage de la mémoire
Dumping de la mémoire physique : Les outils du métier
Analyse d'un vidage de mémoire physique
Comprendre les processus
Analyse du contenu des vidages de mémoire
Mémoire du processus d'analyse syntaxique
Extraction de l'image du processus
Le fichier des pages
Comprendre l'allocation de pools
Médecine légale de la mémoire

Le système de fichiers FAT

Principes de base des graisses
Exploration des enregistrements de démarrage de volume
Exploration des tables d'allocation de fichiers
Exploration des répertoires et des fichiers supprimés
Tout mettre en place
À propos de File Forensics
Explorer les informations cachées
Exploration des signatures de fichiers
Analyse des images montées
Tout mettre en place

Le système de fichiers NTFS

Concepts essentiels de NTFS
Enregistrement d'amorçage du volume NTFS
Le tableau des fichiers maîtres
Exploration des fichiers petits et grands