Tel. +39 02 365738
info@overneteducation.it
www.overneteducation.it

DEFT01

Computer Forensics

Durata: 4 gg

Descrizione

Basato su Deft Linux, il corso sarà concentrato in quattro giornate.
Organizzato in tre aree di competenza:

- •investigazione ed analisi su memorie di massa di sistemi Windows, OS X e Linux
- •investigazione ed analisi su smartphone Android ed Apple
- •Incident Response e gestione dell'incidente informatico

il corso formerà lo studente rendendolo un esperto nell'investigazione applicata ai principali sistemi operativi e al web, padroneggiando le best practices di operatività dei settori specifici grazie a molte ore di pratica applicata direttamente
Obiettivi
L'obiettivo è formare e definire una figura professionale specializzata nel campo dell'investigazione, dell'analisi dei risultati e della produzione di evidenze digitali.

A chi è rivolto?

Liberi professionisti, sistemisti, esperti di sicurezza informatica, forze dell'ordine e militari.

Prerequisiti

- •Conoscenza delle tecnologie di rete locale e geografica
- •Conoscenza ambienti operativi Microsoft e/o Unix/Linux
- •Il corso insegna una metodologia operativa riconosciuta a livello internazionale. Questa metodologia si può adottare sia con software commerciali che con software non commerciali. Per seguire il corso è necessaria una preparazione di base dei sistemi, indipendentemente dal sistema operativo.

Contenuti

Giorno 1:

- •Introduzione alle problematiche di Computer Forensics
- •Breve introduzione al sistema DEFT
- •Preparazione della macchina di analisi e del laboratorio
- •Le 6 fasi operative di un accertamento: individuazione, preservazione, acquisizione, analisi, presentazione delle risultanze e catena di custodia
- •Laboratorio di acquisizione di memorie di massa e memorie ram utilizzando tool per Linux e per Windows
- •Panoramica sull'acquisizione di memorie di massa di cellulari e smarthphone.
- •Approfondimenti sui principali ?le system: fat, ntfs, HFS e HFS+, ext2/3/4, reiserfs, UFS e ZFS
- •Riferimenti temporali e time line dei sistemi
- •Sistemi raid e problematiche di acquisizione

- •Recupero dati - File carving
- •Laboratorio di recupero dati su diversi sistemi

Giorno 2:

- •Architettura dei sistemi operativi Microsoft Windows
- •Architettura dei sistemi Mac OS X
- •Architettura dei sistemi Linux
- •Individuazione delle informazioni di interesse
- •Bash script per la Computer Forensics
- •Laboratorio di analisi dei dati estrapolati
- •Introduzione a DART per le “live forensics”
- •Utilizzo di Bulk extractor
- •Tecniche di anti forensics, occultamento e di distruzione dei dati
- •Cracking di password e creazione di dizionari ottimizzati per attacchi a forza bruta
- •Modello di documentazione per consulenze tecniche
- •Modello di documentazione per la catena di custodia
- •Esercitazioni di laboratorio

Giorno 3:

- •Architettura dei sistemi Android
- •Architettura dei sistemi Apple
- •Rooting e Jailbraking
- •Modalità di acquisizione logica e ?sica
- •Metodogia di analisi
- •Ricerca di informazioni cancellate
- •File carving e recupero dati
- •Laboratorio

Giorno 4:

- •Incident Response su infrastrutture semplici e complesse
- •Modalità operative di intervento in caso di incidente informatico
- •Laboratorio di intervento su macchine compromesse
- •Tecniche di anti forensic, occultamento e di distruzione dei dati
- •Cracking di password e creazione di dizionari ottimizzati per attacchi a forza bruta
- •Tecniche di individuazione di una falsificazione di evidence digitale
- •Modello di documentazione per consulenze tecniche
- •Modello di documentazione per la catena di custodia
- •Modelli di documentazione per la gestione di un incidente informatico
- •Riepilogo argomenti trattati e esempi di domande d'esame