HP Education Services Course Overview

Digital Forensics & Cyber Investigations

Lo scopo del corso è di fornire le nozioni di base riguardo l'investigazione digitale. Al termine del corso i partecipanti saranno in grado di trovare file nascosti, recuperare dati cancellati, duplicare informazioni integre e non ripudiabili con l'utilizzo di tool in aula e analisi di casi studio reali. Il corso è pensato per professionisti del settore informatico interessati ad approfondire le proprie conoscenze sulle procedure teoriche e pratiche di Informatica Forense.

Audience

- Responsabili dei Sistemi Informativi ;
- Forze dell'Ordine;
- Responsabili della Sicurezza Informatica;
- Responsabili di Sistemi di Pagamento;
- Responsabili di Progetti Internet/Intranet;
- Responsabili E-Commerce; Sistemisti e operatori del settore ICT;
- Responsabili EDP e CED; Responsabili di Rete; Amministratori di Rete; Responsabili di Siti Web;
- Studenti Universitari; Consulenti.

Prerequisites

- Aver partecipato al corso HP Enterprise Security Foundation (HL945S) o avere competenze equivalenti;
- Buona conoscenza dei sistemi operativi Windows, Linux;
- Conoscenze di concetti base sui File System, in particolare FAT/FAT32/NTFS/EXT3/EXT4;
- Fondamenti di Networking

Why education services from HP?

- Customized on-site delivery
- Hands-on practice
- Online instructor-led and self-paced training at http://www.hp.com/education

Course Title:	Digital Forensics & Cyber Investigations
HP product number:	U3963S2
Category/Subcategory:	IT Security
Course length:	4 days
Level:	Intermediate
Delivery language:	Italian
Courseware language:	Italian
To order:	Tu puoi ordinare questo corso sul sito: http://www.hp.com/it/formazione scaricare il modulo d'iscrizione e spedirlo a formazione.clienti@hp.com.

- Focus on job-specific skills
- Online instructor-led and self-paced training at http://itresourcecenter.hp.com
- Comprehensive student materials
- State-of-the-art classroom facilities
- Online instructor-led and self-paced training at http://www.hp.com/learn
- Experienced and best-in-the-field HP instructors
- More than 80 training locations worldwide

Detailed course outline

- Panoramica sulle Best Practices
  - L'immodificabilità della fonte di prova ed il metodo scientifico;
  - Analisi live e post mortem (i perché, pro e contro);
  - Identicità della prova
    - hash, cosa sono ed il problema della collisione;
    - catena di custodia;
    - ripetibilità delle operazioni;
  - Digital profiling e social engineering;
- Gli strumenti della C.F. - open source vs commercial;
- Write blocker e hardware forense;
- Le quattro fasi in pratica;
  - Identificazione;
  - Acquisizione;
  - Analisi;
  - Reporting;
- Attività su un pc spento: la checklist delle operazioni da compiere
- Acquisizione di un supporto;
- Il data carving;
- I file di registro di Windows;
- Le tecniche di anti-forensics;
- Cenni sulla steganografia;
- Cenni di Mobile Forensics;
- Cenni sulla legge 48/2008, art. 359 e 360 c.p.p. e DPR 115/02.

Laboratori

GNU/Linux per la Computer Forensics: analisi dei tool - uso della distro C.A.I.N.E. http://www.caine-live.net e/o altre live distro forensi);

- Preview & acquisizione (imaging)
- Acquisizione di un supporto tramite Linux su disco destinazione (DC3DD, AIR, GUYMAGER, DD);
- Acquisizione di un supporto tramite Linux via rete. (dc3dd, dd, netcat);
- Acquisizione di un supporto tramite Windows con FTK Imager;
- Esempio di data carving e come risalire al nome file dal numero di settore;
- Analisi tramite Autopsy e Sleuthkit su un supporto (browsing il filesystem, ricerca per stringhe, recupero dei file cancellati, timeline, ecc.);
- Ricostruzione degli headers tramiter editor esadecimale;
- Analisi dei registri di Windows tramite RegRipper per Windows;
- Analisi dei metadati dei file multimediali;
- Panoramica su altri tools Open Source/Freeware;
- Implementazione di tecniche di anti-forensics;
- Alcuni esempi di cattura di network sniffing ed analisi del PCAP;
- Esercizi pratici e challenges da svolgere in classe.