

Corso e Laboratorio di Sicurezza Informatica e Computer Forensics



Corso pensato per professionisti del settore informatico e tecnico interessati ad approfondire le proprie conoscenze sulla Sicurezza Informatica e sulle procedure teoriche e pratiche di Informatica Forense. Saranno oggetto del corso gli aspetti relativi all'identificazione, al repertaggio corretto delle fonti di prova, all'analisi ed alla presentazione delle conclusioni. Parte pratica di laboratorio, basata sul software Open Source.

A chi e' destinato il corso

- Amministratori di sistema
- Responsabili IT Security
- Consulenti
- Forze dell'ordine
- Studenti universitari
- Personale informatico che intende specializzarsi nel settore della sicurezza informatica e della computer forensics.

Il target

L'obbiettivo del corso è quello di formare personale specializzato nel settore della Sicurezza Informatica, in grado di riconoscere e mitigare gli attacchi informatici, di ricostruirne le dinamiche. Fornire delle solide fondamenta per intraprendere attività nel mondo dell'investigazione digitale, materia in continua trasformazione e divenire. Saranno trattate quindi le tematiche della Computer Forensics anche negli aspetti legali e procedurali su come interfacciarsi col mondo dei tribunali, degli avvocati, come richiedere la liquidazione, come calcolare le vacanze e le differenze tra Perito/CTU e CTP, ecc., in modo da non lasciare solo il tecnico in un ambiente spesso sconosciuto.

Requisiti

Conoscenza del sistema operativo Windows, basi di Linux e dei concetti base sui File System e protocolli TPC/IP.

Durata

2 giornate per un totale di 16 ore divise in 4 sessioni (mattina e pomeriggio).



Indagini Digitali.com
Tel. 0984.1801099 - Fax: 0984.1801244
Web: <http://www.indaginidigitali.com>
E-mail: info@indaginidigitali.com



Dove

Presso aula multimediale attrezzata in Cosenza.

Modalità di iscrizione

Per iscriversi al corso sarà presto disponibile sul sito www.indaginidigitali.com un apposito modulo. L'iscrizione sarà confermata solo in seguito al versamento dell'intera quota.

Nel caso non si raggiunga il numero minimo di partecipanti gli importi saranno restituiti entro un massimo di giorni 10.

Qualsiasi aggiornamento sarà comunque inviato alle email personale inserite nel modulo di iscrizione.

Programma

1 - Penetration test e Vulnerability Assessment

- 1.1 - Gli obiettivi e le regole di ingaggio
- 1.2 - Tipologie di attacco e vulnerabilità
- 1.3 - Il metodo e gli strumenti
- 1.4 - I contenuti del report

2 - Investigare sugli attacchi via web

- 2.1 - Acquisizione dei documenti web
- 2.2 - Ricostruzione degli eventi
- 2.3 - Presentazione dei risultati

3 - Malware Analysis

- 3.1 - Tipologie di malware
- 3.2 - Il reverse engineering
- 3.3 - Strumenti per l'analisi

4 - Simulazioni e casi reali

5 - Panoramica sulle Best Practices

- 5.1 - non modificare la prova
- 5.2 - analisi live e post (i perchè, pro e contro)
- 5.3 - identità della prova
 - 5.3.1 - hash, cosa sono, questione collisioni
 - 5.3.2 - catena custodia, nella teoria e nella realtà
 - 5.3.3 - ripetibilità delle operazioni

6 - Gli strumenti della C.F. - open source vs commerciale

7 - Le quattro fasi (Identificazione, acquisizione, analisi, reporting) in pratica.

8 - GNU/Linux per la C.F.

Docenti

Nanni Bassetti

Consulente Informatico - Fondatore di CFI e Project Manager della GNU/Linux live distro CAINE per la computer forensics. Auditor ISO 27001 di I e II parte.