



Con il patrocinio di



Crimini Informatici

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. **Al termine del corso verrà rilasciato il Certificato di partecipazione ufficiale e la tessera dell'Associazione [World Wide Crime](#) valida per un anno.**

A chi è 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.

Modalità Iscrizione

Per l'iscrizione al corso è necessario compilare il modulo sul sito www.securityside.it/corsi/iscrizione.php Verrà confermata l'iscrizione solo in seguito al versamento della quota entro e non oltre il 25 Febbraio 2010. Il numero massimo di iscritti è di 20 unità.

Requisiti

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

Durata

4 giornate (32 ore) nei giorni 2-3-4-5 Marzo 2010.

Dove

Presso la sala attrezzata dell'Hotel Agathae in via Etna 229, Catania.

Quota di iscrizione

Civili: 650 € + IVA.

Forze dell'ordine: 650 euro IVA inclusa.

Docenti

Gianni Amato

Ricercatore indipendente. Consulente security ed esperto di indagini digitali. Ha esercitato attività di sicurezza informatica per il G8 summit 2009 a L'Aquila.

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.

Denis Frati

Agente della Polizia di Stato e ricercatore indipendente. Fondatore e figura di riferimento di CFI (Computer Forensics Italy), è sviluppatore per la live distro CAINE e autore di svariati tool per la computer forensics. Auditor ISO 27001 di I e II parte.

Eustachio Walter Paolicelli

Titolare dell'omonimo studio legale, presidente dell'associazione World Wide Crime. Specializzato in diritto delle nuove tecnologie e studioso di criminologia. Direttore scientifico di numerosi progetti di ricerca in ambito criminologico e referente dell'Ordine degli Avvocati di Matera alla FIIF presso il CNF.

Indicazioni

Il corso si terrà presso l'Hotel Agathae in via Etnea 229, Catania.

Web: <http://www.hotelagathae.it>

Tel: 095.2500436

I corsisti dovranno presentarsi muniti di portatile e di una pendrive di capienza non inferiore a 2 GB.

I fuori sede potranno usufruire della convenzione stipulata con l'Hotel Agathae alle seguenti condizioni:

- Camera Singola: € 70,00
 - Camera doppia o matrimoniale: € 95,00
- Il costo della camera include WiFi e prima colazione.

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.**

9 - **LABORATORIO**

9.1 - esempio di analisi live ed uso dei tools

9.2 - esempio attività su pc spento

9.3 - preview & acquisizione (imaging)

9.4 - attività di analisi con i tools a disposizione

10 - **Aspetti Legali E Questioni Processuali Della Computer Forensics**

10.1 - Quadro normativo nazionale (Legge 48/2008, ecc.)

10.2 - Caratteristiche e competenze dell'esperto

10.3 - La consulenza tecnica d'ufficio nel processo civile

10.4 - La perizia nel processo penale

10.5 - Il concetto di prova: acquisizione, analisi e conservazione

10.6 - La liquidazione degli onorari

10.7 - Case study: questioni processuali (...*id quod plerumque accidit!*)