



Corso di Holistic Counter-Intelligence

A chi è rivolto:

Tecnici, Sistemisti, Responsabili IT, Giornalisti, Liberi Professionisti, Avvocati, commercialisti, Imprenditori, Manager.

Scopo del corso:

Oggi i crimini digitali sono enormemente facilitati dall'esplosione di internet e dalla semplicità con cui si possono recuperare informazioni praticamente in ogni punto del globo.

Il corso spiega le strategie con cui hacker, crimine organizzato o organizzazioni di intelligence possono violare in generale la privacy delle persone.

Molte sono le insidie di aggressione ai dati e alle comunicazioni, ed è spesso difficile proteggersi dalle tante situazioni di pericolo che possono riguardare sia attività di penetrazione informatica sia attività di intercettazione ambientale e/o pedinamento elettronico.

Il corso ha lo scopo di fornire una vasta panoramica sulle tecnologie e le apparecchiature per la Counterintelligence informatica e ambientale offrendo una difesa "olistica"

alle minacce possibili. Il concetto di difesa olistica passa attraverso un approccio integrato e sinergico di tecniche di sicurezza dei dati e di bonifica ambientale da microspie e segnalatori di ogni tipo attraverso un sistema di tecniche e di protocolli operativo che spiegano quali sono le dinamiche corrette da adottare nella gestione di informazioni delicate.

Durata: 3 giornate - 18 ore

Prerequisti:

Buona conoscenza del sistema operativo e del browser, conoscenza di base di internet

Attrezzatura:

Per lo svolgimento dell'attività didattica è necessario che tutti i discenti abbiano a disposizione un computer collegabile a Internet.

Argomenti:

Introduzione: i rischi per la sicurezza:

- Glossario minimo da conoscere; cenni di elettronica.
- Sicurezza dei dati, anonimato e crittografia
- Sicurezza informatica:
- Crittografia asimmetrica
- Chat crittografate e voip crittografato

La Steganografia e suoi utilizzi:

- Tecniche operative di comunicazione sicura
- Crittografia di supporti fisici (Usb Drive, Hard Disk)
- Email sicure e anonymous Remailer

Sorveglianza audio e video:

- Microspie ambientali, microfoni direzionali (video)
- Microspie indossabili (fare vedere i due cellulari con la segreteria)
- Registratori camuffati, Trasduttore microfonico
- Spy pen, Spy watch,
- Telecamera bottone,
- Occhiali videocamera.
- Spy cam nascoste.

Sorveglianza di movimento

- GPS
- GSM

Controsorveglianza:

Generatore di rumore bianco

Jammer portatile

Wireless Bag

Jammer GPS

Rivelatore di microspie e di videocamere (con cellulare)

Termocamere

Fotografia infrarossa e ultravioletta

Analizzatore di spettro

Analizzatore linea telefonica

Docenti:

Leonida Reitano

Dottore di ricerca in sociologia della comunicazione e McLuhan fellow dal febbraio 2003. Esperto nazionale di Open Source Intelligence (OSINT) e Personal Digital Security. E' autore del primo manuale italiano di Open Source Intelligence: Esplorare Internet, manuale di investigazioni digitali e Open Source Intelligence.

Salvatore Merlino

Esperto nazionale di strumenti di intelligence e counter intelligence elettronica con una solida esperienza nel mondo delle istituzioni.

Contatti:

Leonida Reitano

3899280813

agi@fastmail.fm

Ndr. il corso ha il solo obiettivo di formare le conoscenze necessarie alla difesa da attività di penetrazione informatica, di attività di intercettazione ambientale e/o pedinamento elettronico perpetrate in modo illecito.