

## GESTIONE DEGLI INCIDENTI INFORMATICI

6 CFU

Semestre: II

SSD: INF/01

Codice Insegnamento: F54075

### Programma

1. Introduzione. Principi di gestione degli incidenti informatici: Politiche di sicurezza, programma di classificazione delle informazioni. Definizioni di Incidente informatico e di Digital forensics
2. Incidenti informatici. Classificazione, definizione degli attacchi più comuni. Procedure da adottare a livello tecnico ed organizzativo. Tools di fist recovery, preparazione di un team di gestione degli incidenti informatici.
3. Principi di Log analysis. Struttura di un log, metodiche di lettura, strumenti di acquisizione, validazione ed analisi dei log, tecniche di correlazione e di mantenimento dell'integrità dei log. Architetture di logging.
4. Sistemi di Logging a livello sistema. Definizione ed individuazione dei meccanismi di logging in ordine ai sistemi operativi. Logging sotto Linux e Windows 2000. Logging sotto Windows XP. Cenni al logging di sistema di Sun Solaris.
5. Sistemi di Logging a Livello Rete. Router syslog. Analisi dei formati di log di router CISCO e di altri vendors. Analisi dei log, esame degli strumenti TCPDump, Ethereal e similari
6. Sistemi di Intrusion Detection. Snort, principi di funzionamento e installazione. Esempi di regole di sicurezza e di packet analysis. Gestione e management dei sistemi basati su NIDS.
7. Advanced Log Analysis: riconoscimento degli attacchi più comuni a seguito di analisi dei pacchetti di SNORT/TCPDUMP.
8. First Incident Response: operazioni di riconoscimento dei segni indicativi di attacco ricevuto, ripristino, individuazione dei punti di entrata, backtracing, incident management.
9. Digital Forensic: Definizione di File Systems, Slack Space, altri possibili repository di files o frammenti. Metodiche di acquisizione dei dati a seguito di attacco e di altri episodi criminosi che richiedono l'intervento di un forensic examiner.
10. Crittografia applicata all'integrità dei files: effettuazione delle immagini dei dischi e utilizzo dei software per la firma digitale ed il controllo dell'integrità dei files. Algoritmi Md5 e SHA-1. Differenze e best practices.
11. Ricerca di files e informazioni sui supporti acquisiti – Forensic Analysis. Teoria e pratica dell' utilizzo degli strumenti di informatica forense, con i sistemi operativi Windows e Linux. Esame delle prove, presentazione dei risultati, ripetibilità, best practices.
12. Operazioni legali. Applicazione dei principi legali del codice penale e di procedura penale e leggi correlate alle operazioni di gestione degli incidenti – Cenni. Modulistica operativa.

### Materiale di riferimento

Dario Forte/Luca de Grazia: Manuale di Infosecurity Management: [www.degrazia.it](http://www.degrazia.it) – Al momento dell'acquisto menzionare l'appartenenza al DTI

### Materiale consigliato

Progetto IRITALY: documenti e tools di incident response e informatica forense – [www.iritaly.org](http://www.iritaly.org)

### Prerequisiti

Conoscenza di base della suite tcp ip

Conoscenza di base dei sistemi operativi Windows 2000, XP e Linux

### Modalità di valutazione

Esame scritto + esame orale.

### Incompatibilità con altri insegnamenti

Nessuna

**Pagina web del corso:** [http://www.dti.unimi.it/corsi/gestione\\_incidenti\\_informatici](http://www.dti.unimi.it/corsi/gestione_incidenti_informatici)