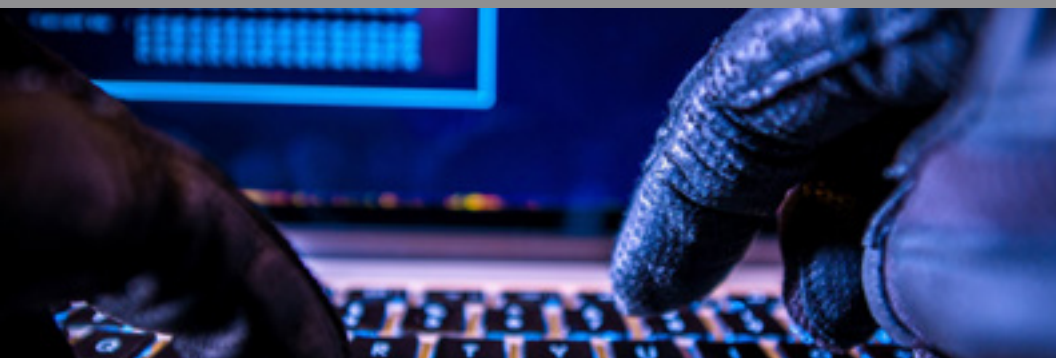


SUPSI

Digital Forensics for Blockchain Analysis, Penetration Testing and Incident Response

Certificate of Advanced Studies
2a edizione 2018/19



Advanced Studies⁺

La formazione continua universitaria

Sempre più in azienda sono necessarie competenze specifiche in grado di far fronte ai frequenti attacchi informatici che mettono a dura prova i crismi di sicurezza. Disporre di un team di tecnici adeguatamente preparati a gestire i processi di valutazione della sicurezza di un sistema o di un'infrastruttura critica, tipicamente riconducibili alle attività di Penetration Testing, diventa cruciale ai fini di evidenziare per tempo le debolezze dell'infrastruttura e le vulnerabilità che ne hanno permesso l'accesso non autorizzato. Ma è soltanto una componente di un filiera complessa che tecnici informatici, amministratori di rete e sistemisti devono conoscere per fronteggiare i sempre più frequenti attacchi informatici moderni. Un secondo argomento prende in considerazione le attività di Incident Response, fondamentali per gestire e affrontare correttamente e tempestivamente le conseguenze dovute alla violazione della sicurezza di un attacco informatico. Saper definire un piano di risposta agli attacchi consente all'azienda di limitare i danni, ridurre i tempi e i costi di intervento e soprattutto di garantire il corretto funzionamento del business aziendale. Un terzo argomento trattato nel corso riguarda l'apprendimento e l'analisi delle tecniche di analisi delle crypto valute. Tutti i moduli includono lezioni mirate su aspetti legali che accompagnano e contraddistinguono i temi trattati nei singoli moduli.

Obiettivi

Il corso consente di acquisire nuove e avanzate conoscenze per:

- ♦ apprendere le tecniche di analisi e gestione delle crypto valute;
- ♦ apprendere le tecniche e gli approcci per effettuare correttamente dei Penetration Testing di infrastruttura critica;
- ♦ apprendere le tecniche e le attività di intervento fondamentali per la gestione di un Incident Response da impiegare in caso di attacco informatico.

Destinatari

Il corso si rivolge ai professionisti del settore ICT che si occupano della manutenzione della sicurezza informatica o hanno il compito di gestire le emergenze in seguito a un incidente informatico in cui sono coinvolte le nuove tecnologie e i rispettivi dati aziendali, come per esempio tecnici informatici, amministratori di rete, periti e consulenti informatici.

Requisiti

Il corso richiede la conoscenza dei paradigmi di almeno un linguaggio di programmazione.

Certificato

Attestato di frequenza.

Per coloro che superano gli esami previsti in ciascun modulo : Certificate of Advanced Studies SUPSI in Digital Forensics for Blockchain Analysis, Penetration Testing and Incident Response.

Crediti di studio

11 ECTS

Programma

Modulo 1

Penetration Testing – 48 ore-lezione, 4 ECTS

Parte tecnica

- ♦ Penetration testing fundamentals.
- ♦ Information Gathering and target Enumeration.
- ♦ Web applications attack and exploitation.
- ♦ Software exploitation fundamentals.
- ♦ Client Side Attack.
- ♦ Maintaining access and lateral movement.
- ♦ Attacking the network layer.

Aspetti legali

- ♦ Introduzione al diritto informatico e di internet.
- ♦ Lotta internazionale contro la cyber criminalità.
- ♦ Diritto penale informatico e relative casistiche.
- ♦ Gli strumenti processuali civili e penali.
- ♦ Sorveglianza preventiva, sorveglianza repressiva.

Modulo 2

Incident Response – 36 ore-lezione, 3 ECTS

Parte tecnica

- ♦ Definizione di "incident" e le sei fasi fondamentali.
- ♦ Creazione di un piano di incident response (preparazione).
- ♦ Identificazione di un "incident".
- ♦ Investigazione durante le fasi di incident: isolamento e acquisizione delle informazioni (contenimento ed estirpazione)
- ♦ Ripristino delle risorse (recupero).
- ♦ Creazione di un report sull'incident e sulle attività svolte (lezione appresa).
- ♦ Pianificazione per il recupero del disastro attraverso esempi concreti.
- ♦ Pianificazione per la continuità del business attraverso esempi concreti.

Aspetti legali

- ♦ Privacy e dati personali quali risorse e limiti d'azione.
- ♦ Cyber sorveglianza sul luogo di lavoro.
- ♦ Organizzazione aziendale adeguata, obbligo di prevenzione.
- ♦ Difesa e attacco in diritto civile e penale.
- ♦ Casi pratici di furto di dati e reazione corretta.

Modulo 3

Blockchain Analysis – 48 ore-lezione, 4 ECTS

Parte tecnica

- ♦ Le Blockchain: funzionamento, pregi e limiti.
- ♦ Crittografia: funzioni crittografiche di hash e firma digitale
- ♦ Introduzione alle transazioni Bitcoin ed il loro linguaggio
- ♦ Approfondimento della Blockchain in riferimento alle transazioni ed ai meccanismi di sicurezza e protezione contro le frodi
- ♦ Conservazione delle chiavi: wallet software, e-wallet e hardware wallet
- ♦ Costruzione manuale di una transazione
- ♦ Transazioni complesse con più input ed output. Cenni sui meccanismi multi-signature e su altri meccanismi avanzati

Aspetti legali

- ♦ La nuova legge federale sulla firma digitale (1.1.2017)
- ♦ Responsabilità in caso di perdita delle credenziali d'accesso
- ♦ Algoritmi e proprietà intellettuale
- ♦ Crypto valute e legislazione bancaria e finanziaria
- ♦ I contratti del mondo IT
- ♦ Esempi pratici

Durata

132 ore-lezione

Relatori

Professionisti con esperienze significative nel proprio ambito d'insegnamento.

Responsabile

Dr. Alessandro Trivilini, responsabile Laboratorio informatica forense SUPSI

Iscrizioni

Entro il 31 agosto 2018.

Date

Modulo 1

20, 27 settembre, 4, 11, 18, 25 ottobre, 8, 15, 22, 29 novembre, 6, 13 dicembre 2018
esame: 20 dicembre 2018

Modulo 2

10, 17, 24, 31 gennaio, 7, 14, 21, 28 febbraio, 14 marzo 2019
esame: 21 marzo 2019

Modulo 3

4, 11, 18 aprile, 2, 9, 16, 23, 29 maggio, 5, 6, 12, 13 giugno 2019
esame: 18 giugno 2019

Orari

Giovedì 17.30-21.00

Nelle seguenti date le lezioni termineranno alle ore 19.30: 20 dicembre 2018, 21 marzo e 18 giugno 2019

Luogo

SUPSI, Dipartimento tecnologie innovative, Manno.

Costo

CHF 7'000.—

Osservazioni

Il numero di partecipanti è limitato a 12.



Informazioni

SUPSI, Dipartimento tecnologie innovative
Galleria 2, Via Cantonale 2c, CH-6928 Manno
T +41 (0)58 666 65 89, F +41 (0)58 666 65 71
dti.fc@supsi.ch, www.supsi.ch/dti/forense

