Insegnamento	Sicurezza dei Sistemi
Livello e corso di studio	Laurea Magistrale in Ingegneria Informatica (LM32)
Settore scientifico disciplinare (SSD)	ING-INF/05
Anno di corso	1
Numero totale di crediti	9
Propedeuticità	-
Presentazione	Il Corso di Sicurezza dei Sistemi ha lo scopo di far acquisire allo studente una buona conoscenza dei principi che governano la sicurezza dei sistemi di elaborazione. Il Corso propone i concetti basilari nell'ambito della sicurezza dei sistemi di elaborazione, e li declina nello studio delle tecniche di crittografia e la loro applicazione ai vari aspetti della sicurezza informatica. Inoltre, obiettivo formativo del Corso è fornire allo studente una conoscenza nel dettaglio sul funzionamento dei principali protocolli alla base della progettazione di sistemi distribuiti sicuri. Le Etivity associate al Corso sviluppano le competenze necessarie ad analizzare protocolli di sicurezza e vulnerabilità informatiche attraverso l'impiego di appositi strumenti ed ambienti al calcolatore.
Obiettivi formativi	Il Corso di Informatica ha i seguenti obiettivi formativi: 1. Illustrare i concetti di base nell'ambito della sicurezza dei sistemi di elaborazione 2. Illustrare le principali tecniche di crittografia 3. Illustrare l'applicazione della crittografia in ambito informatico 4. Illustrare i principali protocolli di sicurezza nei sistemi distribuiti
Risultati di apprendimento attesi	**Conoscenza e capacità di comprensione** Lo studente al termine del Corso avrà conoscenza delle metodologie per affrontare problematiche legate alla sicurezza dei sistemi di elaborazione delle informazioni. Inoltre, lo studente acquisirà la capacità di analizzare protocolli ed applicazioni di autenticazione, sicurezza della posta elettronica e del Web, e tutti gli aspetti legati alla sicurezza dei sistemi informatici. Lo studente verrà infine reso in grado di confrontare le conseguenze derivanti dalle scelte architetturali da prendere nella progettazione di un sistema informativo sicuro. Inoltre, tramite le Etivity gli studenti acquisiranno la capacità di analizzare vulnerabilità di sistemi informativi, e testarne la permeabilità alle intrusioni, all'interno di ambienti di analisi forense e testing per la sicurezza informatica come Kali. **Applicazione delle conoscenze** Lo studente sarà in grado di applicare conoscenze e metodologie per collaudare, progettare e realizzare sistemi informatici sicuri che facciano uso delle tecniche e degli strumenti analizzati durante il corso. Le Etivity prevedono l'applicazione delle conoscenze teoriche a problemi pratici, come simulare attacchi e risolvere vulnerabilità, da risolvere con l'ausilio di ambienti di analisi forense e testing per la sicurezza informatica (Kali). **Capacità di trarre conclusioni** Lo studente avrà acquisito una metodologia di analisi dei meccanismi che garantiscono la sicurezza di un sistema informatico; sarà, inoltre, in grado di giudicare la validità di progetti di sistemi sicuri per l'elaborazione delle informazioni. Infine, lo studente sarà in grado di effettuare ricerche bibliografiche, di analizzare ed interpretare le fonti rilevanti, al fine di analizzare nuovi protocolli di sicurezza. **Abilità comunicative** Lo studente sarà in grado di descrivere e sostenere conversazioni su tematiche relative a problematiche complesse legate alla sicurezza dei sistemi informatici di elaborazione delle informazioni e delle reti, adoperando una terminologia adeguata. **Capacità di apprendere** Lo studente al termine del Corso avrà conoscenza delle nozioni fondamentali necessarie per affrontare in autonomia qualsiasi problematica relativa alla sicurezza dei sistemi informatici e di rete. Sarà in grado di indagare sulle tecniche di crittografia dei dati, di firma digitale, di autenticazione, di integrità e di non ripudiabilità.

Prerequisiti	La frequenza al Corso richiede la **conoscenza** dei concetti fondamentali di **networking** e **sistemi operativi** come appresi nel Corso di Reti di Calcolatori (L8), e nel Corso di Sistemi Operativi (L8), rispettivamente. Al riguardo, si consiglia di rivedere tali nozioni, propedeutiche per l'apprendimento e l'approfondimento della sicurezza a livello di rete e del Web, e nei sistemi operativi.
Organizzazione dell'insegnamento	Il Corso è sviluppato attraverso le **lezioni preregistrate audio-video** che compongono, insieme a slide e dispense, i materiali di studio disponibili in piattaforma. Sono poi proposti dei **test di autovalutazione**, di tipo asincrono, che corredano le lezioni preregistrate e consentono agli studenti di accertare sia la comprensione, sia il grado di conoscenza acquisita dei contenuti di ognuna delle lezioni. La **didattica interattiva** è svolta nel forum della "classe virtuale" e comprende **4 Etivity** che declinano le conoscenze acquisite nelle lezioni di teoria e durante le esercitazioni in esempi concreti di analisi e collaudo relativamente alla sicurezza di sistemi informatici e di rete. In particolare, il Corso di Sicurezza dei Sistemi prevede 9 Crediti formativi. Il carico totale di studio per questo modulo di insegnamento è di circa 225 ore così suddivise in: ● circa 170 ore per la visualizzazione e lo studio del materiale videoregistrato; ● circa 50 ore di Didattica Interattiva per l'elaborazione e la consegna di 4 Etivity; ● circa 5 ore di Didattica Interattiva per l'esecuzione dei test di autovalutazione.
Contenuti del corso	**Modulo 1 – Reti, Hashing (impegno di 19 ore)** dove sono affrontati i seguenti argomenti: Sicurezza delle Reti, Autenticazione dei messaggi e funzione SHA-1. Esercitazioni su funzioni hash crittografiche. **Modulo 2 - MAC e firme (impegno di 24 ore)** dove sono affrontati i seguenti argomenti: Codici di autenticazione dei Messaggi, Firma Digitale. Esercitazioni su Codici di autenticazione dei Messaggi e su Firma Digitale. **Modulo 3 – Kerberos (impegno di 10,5 ore)** dove sono affrontati i seguenti argomenti: Applicazioni di autenticazione: Kerberos. **Etivity 1 (15 ore di carico di studio)** – Laboratorio di crittografia. **Modulo 4** – **Web (impegno di 38 ore)** dove sono affrontati i seguenti argomenti: Sicurezza della posta elettronica, Sicurezza a livello rete, Sicurezza Web, Firewall. Esercitazione su sicurezza Web e Firewall. **Modulo 5** – **Sistemi, Wireless (impegno di 24 ore)** dove sono affrontati i seguenti argomenti: Sicurezza dei sistemi Informatici, Sicurezza delle Reti Wireless. Esercitazione su protocolli di sicurezza. **Etivity 2 (15 ore di carico di studio)** – Network mapping. **Modulo 6** – **Autenticazione, AC (impegno di 15,5 ore)** dove sono affrontati i seguenti argomenti: User Authentication, Access Control. Esercizi su user authentication. **Modulo 7** – **DB, DC, IDS (impegno di 17,5 ore)** dove sono affrontati i seguenti argomenti: Database and Datacenter Security, Malicious Software, IDS. **Etivity 3 (15 ore di carico di studio)** – Analisi vulnerabilità e penetration testing. **Modulo 8** – **OS, Cloud, IoT (impegno di 17,5 ore)** dove sono affrontati i seguenti argomenti: Software Security, Operating System Security, Cloud ed IoT Security. **Esercitazioni su compiti d'esame (2 lezioni di esercitazione per un impegno di 5 ore)** **Etivity 4 (6 ore di carico di studio)** – Simulazione esame.
Materiali di studio	· MATERIALI DIDATTICI A CURA DEL DOCENTE Il materiale didattico presente in piattaforma è suddiviso in 8 moduli. Essi ricoprono interamente il programma e ciascuno di essi contiene dispense, slide e videolezioni in cui il docente commenta le slide. Tale materiale contiene tutti gli elementi necessari per affrontare lo studio della materia. Testi consigliati: W. Stallings – Cryptography and Network Security, 7th Ed., Pearson W. Stallings – Computer security: principles and practice, 4th Ed., Pearson
Modalità di verifica dell'apprendimento	L'esame consiste nello svolgimento di una **prova scritta** tendente ad accertare le capacità di analisi e rielaborazione dei concetti acquisiti e di una **serie di attività** (**e-tivity**) svolte durante il Corso nelle **classi virtuali**.

	I risultati di apprendimento attesi circa le conoscenze della materia e la capacità di applicarle sono valutate dalla prova scritta, mentre le abilità comunicative, la capacità di trarre conclusioni e la capacità di autoapprendimento sono valutate in itinere attraverso le e-tivity.
Criteri per l'assegnazione dell'elaborato finale	L'assegnazione dell'**elaborato finale** avverrà sulla base di un colloquio con il docente in cui lo studente manifesterà i propri specifici **interessi** in relazione a qualche argomento che intende approfondire; non esistono **preclusioni** alla richiesta di assegnazione della tesi e non è prevista una **media particolare** per poterla richiedere.