UNIVERSITÀ DEGLI STUDI DI PALERMO

DIPARTIMENTO	Ingegneria
ANNO ACCADEMICO OFFERTA	2021/2022
ANNO ACCADEMICO EROGAZIONE	2021/2022
CORSO DILAUREA MAGISTRALE	INGEGNERIA DEI SISTEMI CIBER-FISICI PER L'INDUSTRIA
INSEGNAMENTO	CYBERSECURITY
TIPO DI ATTIVITA'	C
AMBITO	20917-Attività formative affini o integrative
CODICE INSEGNAMENTO	19220
SETTORI SCIENTIFICO-DISCIPLINARI	ING-INF/05
DOCENTE RESPONSABILE	FERRARO PIERLUCA Ricercatore a tempo determinato Univ. di PALERMO
ALTRI DOCENTI	
CFU	6
NUMERO DI ORE RISERVATE ALLO STUDIO PERSONALE	96
NUMERO DI ORE RISERVATE ALLA DIDATTICA ASSISTITA	54
PROPEDEUTICITA'	
MUTUAZIONI	
ANNO DI CORSO	1
PERIODO DELLE LEZIONI	1° semestre
MODALITA' DI FREQUENZA	Facoltativa
TIPO DI VALUTAZIONE	Voto in trentesimi
ORARIO DI RICEVIMENTO DEGLI STUDENTI	**FERRARO PIERLUCA** Martedì 15:00 17:00 Edificio 6, terzo piano

DOCENTE: Prof. PIERLUCA FERRARO

PREREQUISITI	Informatica di Base
RISULTATI DI APPRENDIMENTO ATTESI	Conoscenza e capacita' di comprensione (knowledge and understanding): Lo studente, al termine del corso, avra' acquisito conoscenze e metodologie per affrontare problematiche legate alla sicurezza dei sistemi e delle Infrastrutture informatiche. Lo studente sara' in grado di analizzare protocolli ed applicazioni di autenticazione, e tutti gli aspetti legati alla sicurezza dei sistemi informatici. Conoscenza e capacita' di comprensione applicate (applying knowledge and understanding): Lo studente avra' acquisito conoscenze e metodologie per realizzare sistemi informatici sicuri che facciano uso delle tecniche e degli strumenti analizzati durante il corso. Autonomia di giudizio (making judgements): Lo studente avra' acquisito una metodologia di analisi dei meccanismi che garantiscono la sicurezza di un sistema informatico e sara' in grado di giudicare la validita' di progetti di sistemi sicuri per l'elaborazione delle informazioni. Abilita' comunicative (communication skills): Lo studente sara' in grado di discutere con competenza e proprieta' di linguaggio problematiche complesse legate alla sicurezza dei sistemi informatici di elaborazione delle informazioni e delle reti. Capacita' di apprendere (learning skills): Lo studente sara' in grado di affrontare con autonomia qualsiasi problematica relativa alla sicurezza dei sistemi informatici.
VALUTAZIONE DELL'APPRENDIMENTO	Le conoscenze e le competenze acquisite dallo studente saranno verificate attraverso una prova scritta (prova in itinere + prova finale o prova complessiva) e un colloquio orale. Valutazione della prova scritta Durante il corso, in accordo con il calendario accademico, sara' possibile sostenere una prova in itinere. Tale prova, a discrezione dell'allievo potra' essere completata con una prova finale da sostenere nel periodo compreso tra la fine delle lezioni ed il primo appello del corso. La media pesata della prova in itinere e di quella finale costituisce il voto della prova scritta. La prova scritta (in itinere + finale o complessiva) e' costituita da almeno tre esercizi volti a verificare le conoscenze dello studente degli argomenti affrontati durante il corso, e di applicare le capacita' e le conoscenze acquisite. Nello svolgimento assume fondamentale importanza il commento teorico dei risultati ottenuti. L'articolazione della soluzione consente di apprezzare tutti i livelli di preparazione. La valutazione e' espressa in trentesimi ed un minimo di 15 e' richiesto per accedere alla prova orale. Valutazione per la prova orale La prova orale consiste in un colloquio, volto ad accertare il possesso delle competenze e delle conoscenze disciplinari previste dal corso; la valutazione viene espressa in trentesimi. Durante il colloquio orale lo studente dovra' essere in grado di discutere le soluzioni proposte durante la prova scritta; inoltre saranno proposte domande di diverso e crescente livello di complessita' al fine di valutare il raggiungimento degli obiettivi formativi e le abilita' comunicative dello studente. Infine, allo scopo di valutare l'autonomia di giudizio, sara' richiesto di analizzare le caratteristiche di specifici scenari applicativi e di proporre le soluzioni piu' adeguate ai problemi individuati. La valutazione finale terra' conto sia del punteggio della prova scritta (50%) che di quello delle prova orale (50%). Eccellente 30-30 e lode. Durante entrambe le prove lo studente dovra' dimostrare padronanza completa degli argomenti del corso. Durante il colloquio orale l'allievo dovra' dimostrare la maturita' di saper collegare i diversi aspetti trattati e la capacita' di saper generalizzare. Dovra' mostrare autonomia nella soluzione dei quesiti e la capacita' di individuare le informazioni necessarie per la soluzione degli stessi. Molto buono 27-29 Buona padronanza degli argomenti, lo studente e' in grado di applicare le conoscenze per risolvere i problemi proposti. Buono 24-26 buona conoscenza dei principali, discreta padronanza e proprieta' di linguaggio, con capacita' di applicare autonomamente le conoscenze alla soluzione dei problemi proposti. Discreto 21-23 Piu' che sufficiente padronanza degli argomenti principali dell'insegnamento, limitata capacita' di applicare autonomamente le conoscenze acquisite. Sufficiente 18-20 conoscenza di base degli argomenti principali dell'insegnamento e del linguaggio tecnico. Insufficientenon possiede una conoscenza accettabile dei contenuti degli argomenti trattati nell'insegnamento.
OBIETTIVI FORMATIVI	Il corso si propone di fornire allo studente i concetti di base nell'ambito della sicurezza dei sistemi di elaborazione. Durante il corso sono affrontate le problematiche relative alla sicurezza degli impianti informatici in generale.

ORGANIZZAZIONE DELLA DIDATTICA	Lezioni frontali i in aula
TESTI CONSIGLIATI	Dispense fornite dal docente.

PROGRAMMA

ORE	Lezioni
6	LA SICUREZZA DEI SISTEMI INFORMATICI: CONCETTI GENERALI La sicurezza informatica, servizi, meccanismi e attacchi alla sicurezza. Autenticazione Riservatezza dei dati Integrità dei dati Controllo degli accessi Non ripudiabilità Disponibilità del servizio.
10	Elementi di crittografia sistemi crittografici tradizionali, la crittografia asimmetrica. Cifratura simmetrica e riservatezza dei dati Crittografia a chiave pubblica e autenticazione dei dati
6	GARANZIA DELLA RISERVATEZZA La firma digitale e il documento informatico, la normativa di riferimento in materia di firma digitale, Rischi e pericoli, gli svantaggi e le vulnerabilita della firma digitale, i possibili attacchi informatici ai documenti firmati digitalmente. Rimedi e contromisure.
10	SICUREZZA INFORMATICA nei grandi impianti Il contesto di riferimento, ambito normativo, Il codice dell'Amministrazione Digitale e successive modificazioni La politica di sicurezza nelle pubbliche amministrazioni, dall'analisi del rischio agli audit di sicurezza: le fasi del ciclo di gestione della sicurezza informatica. Business Continuity Management e Disaster Recovery, Le figure dei responsabili del processo di gestione della sicurezza.
10	CRIMINI CIBERNETICI Tipologie di crimini informatici Furto della proprieta' intellettuale, Furto di altre informazioni proprietarie (dati finanziari personali, ecc.), Attacchi di DOS, Virus, worms e altri codici malevoli, spyware, Frodi, Furto di identita, Generazione illegale di messaggi di posta elettronica, Phishing, Acceso ed uso non autorizzato dei sistemi e delle reti, Sabotaggio, Estorsioni, alterazione di siti web, macchine zombie, crimini legati al sesso: pedopornografia, diffusione non autorizzata di materiale privato.

ORE	Esercitazioni
12	Esercitazioni al computer