Principali informazioni sull'insegnamento	**A.A. 2020-2021**
Titolo insegnamento	Sicurezza Informatica
Corso di studio	Informatica e Comunicazione Digitale
Crediti formativi	6 CFU
Denominazione inglese	Computer Security
Obbligo di frequenza	NO
Lingua di erogazione	Italiano

Docente responsabile	Nome Cognome	Indirizzo Mail
	Danilo Caivano	danilo.caivano@uniba.it
Luogo e Orario di Ricevimento	Dip. Informatica Sede Taranto Stanza Docenti	Dal 28 settembre 2020 al 13 gennaio 2021 Giovedì dalle ore 12:30 alle ore 13:30 Altri periodi: per appuntamento

Dettaglio credi formativi	Ambito disciplinare	SSD	Crediti
Lezioni Frontali	Informatico	ING/01	4
Esercitazioni	Informatico	ING/01	1
Progetto	Informatico	ING/01	1

Modalità di erogazione	
Periodo di erogazione	I semestre
Anno di corso	III anno
Modalità di erogazione	Lezioni frontali Esercitazioni Progetto

Organizzazione della didattica	
Ore totali	150
Ore di corso	48
Ore di studio individuale	102

Calendario	
Inizio attività didattiche	28 Settembre 2020
Fine attività didattiche	13 Gennaio 2021

Syllabus	
Prerequisiti	Prerequisiti definiti dal manifesto del corso di studi
Risultati di apprendimento previsti (declinare rispetto ai Descrittori di Dublino) (si raccomanda che siano coerenti con i risultati di apprendimento del CdS, riportati nei quadri A4a, A4b e A4c della SUA, compreso i risultati di apprendimento trasversali)	• *Conoscenza e capacità di comprensione* Il principale risultato di apprendimento atteso è la conoscenza relativa a processi, metodi e tecniche per l'analisi e la gestione di un incidente di sicurezza supportati da strumenti allo stato della pratica. Lo studente acquisisce tale conoscenza sia attraverso le lezioni frontali e la partecipazione a seminari tematici

	erogati durante il corso, sia attraverso esercitazioni che gli consente di mettere in pratica e verificare quanto appreso, acquisendo così consapevolezza della capacità di comprensione e di come migliorare l'applicazione delle tecniche apprese. • *Conoscenza e capacità di comprensione applicate* Al fine di consentire agli studenti di applicare le conoscenze acquisite, essi eseguono sia esercizi individuali che collaborative. Inoltre, sono tenuti a sviluppare un progetto in cui applicano alcune delle tecniche presentate in aula, dopo aver selezionato quelle più appropriate per il caso specifico. Questo progetto contribuisce alla valutazione finale dello studente e quindi al voto finale d'esame. • *Autonomia di giudizio* Obiettivo del corso è che lo studente raggiunga una significativa autonomia nel valutare i pericoli inerenti le vulnerabilità di sistemi informatici. Le esercitazioni che si svolgono durante il corso contribuiscono al raggiungimento di tale autonomia grazie anche alla discussione di tali scelte con il docente. L'autonomia di giudizio è parte della valutazione finale dello studente e tiene conto delle discussioni avvenute durante le lezioni, delle esercitazioni e della presentazione del progetto. • *Abilità comunicative* Comunicare ed esprimere verbalmente in modo chiaro ed efficace le conoscenze apprese, presentare casi applicativi ed esempi illustrativi. Discutere le soluzioni adottate nello sviluppo del caso di studio. • *Capacità di apprendere* Individuare, elaborare e organizzare informazioni appropriate per soluzioni di problemi connessi alle minacce di sicurezza informatica.
Contenuti di insegnamento	**Introduzione** • Scenario Cyber • Pattern di attacco • Cyber Kill Chain **Concetti fondamentali** • Asset • Threat • Threat agent • Threat intelligence • Vulnerabilità • Rischio • Exploit • Attacco • Mitigazione e controllo • CIA Triade: Confidenzialità, Integrità e Disponibilità

	Access Control
	• Subject e Object
	• Processi
	  o Identificazione
	  o Autenticazione
	  o Autorizzazione
	  o Accounting
	• Ruoli e responsabilità
	• Tipologie di Access Control
	• Modelli di Access Control
	Sicurezza in rete
	• Fondamenti di Networking
	  o Classificazione delle reti
	  o Come Funzionano le reti
	  o Elementi che costituiscono una rete
	  o Modello TCP/IP
	  o Modello OSI
	  o Internet Protocol
	• Dispositivi di sicurezza di rete
	  o Firewall
	  o Intrusion Detection System
	  o Intrusion Prevention System
	  o Anomaly Detection System
	  o Advanced Malware Protection
	Sicurezza Organizzativa
	• Security lifecycle
	• Security Controls
	• Security Organizational Unit
	  o Security Operation Center
	  o Computer Security Incident Response Team
	  o Support Unit
	Sicurezza Applicativa
	• Privacy by Design
	• Security by Design
	• Strumenti e tecniche per lo sviluppo di software orientato alla privacy e alla sicurezza
	• Attacchi: tecniche e contromisure
	  o SQL Injection
	  o Cross-Site Scripting (XSS)
	  o XML Injection
	  o File Inclusion
	  o Broken Authentication
	  o Session Management
	  o Sensitive Data Exposure
	  o Cross Site Request Forgery
	  o Insecure Direct Object References
	Penetration Testing and Security Auditing: Kali Linux
	Port Scanning: Nmap

Programma	
Testi di riferimento	• Omar Santos, Joseph Muniz, Stefano De Crescenzo, "CCNA Cyber Ops SECFND 210-250", Cisco Systems; Har/Psc edizione (3 aprile 2017) • Kali Linux, "Official Documentation" https://www.kali.org • Nmap Network Scanning, "The Official Nmap Project Guide to Network Discovery and Security Scanning", ISBN: 978-0-9799587-1-7. https://nmap.org/book/toc.html
Note ai testi di riferimento	I testi di riferimento sono integrati con slide, dispense del docente e altro materiale didattico messi a disposizione degli studenti sulla piattaforma di e-learning usata dal CdS.
Metodi didattici	• Lezioni frontali • Esercitazioni • Seminari
Metodi di valutazione (indicare almeno la tipologia scritto, orale, altro)	La verifica dei risultati formativi raggiunti avviene durante l'esame, che prevede un colloquio orale che illustra e discute il progetto sviluppato in gruppo e gli argomenti trattati a lezione. Il progetto deve essere consegnato 3 giorni lavorativi prima della data dell'esame.
Criteri di valutazione (per ogni risultato di apprendimento atteso su indicato, descrivere cosa ci si aspetta lo studente conosca o sia in grado di fare e a quale livello al fine di dimostrare che un risultato di apprendimento è stato raggiunto e a quale livello)	Per accertare le conoscenze acquisite dallo studente, e anche la sua autonomia di giudizio, le capacità comunicative e la capacità di apprendere, è prevista una valutazione, attraverso una presentazione orale, del progetto svolto (in gruppo) considerando come è stato strutturato, come sono stati applicati i principi e le metodologie, l'adeguatezza delle tecniche utilizzate, l'originalità delle soluzioni, la chiarezza e la capacità di sintesi che risulta dalla documentazione prodotta (relazione scritta, orale e presentazione tramite diapositive). Sarà valutato il contributo del singolo studente al lavoro di gruppo. La valutazione è in trentesimi ed è la stessa per tutto il gruppo di lavoro. La valutazione individuale è quindi ottenuta con punti bonus o malus in relazione a: il contributo dato al gruppo nella realizzazione del progetto; alla capacità di sintesi e chiarezza di esposizione; alla capacità di analisi dei pericoli inerenti le minacce di sicurezza informatica e di riportare il proprio giudizio critico; alla padronanza dei termini tecnici.
Altro	