Denominazione	SISTEMI OPERATIVI E CYBERSECURITY
Moduli componenti	-
Settore scientifico-disciplinare	IINF-05/A
Anno di corso e semestre di erogazione	3° anno, 2° semestre
Lingua di insegnamento	Italiano
Carico didattico in crediti formativi universitari	9
Numero di ore di attività didattica frontale	72 (pari a 9 CFU di didattica erogativa)
Docente	Docente da reclutare
Risultati di apprendimento specifici	l corso mira a fornire agli studenti una solida comprensione dei costrutti base per comprendere il funzionamento di un Sistema Operativo (SO) general-purpose e le nozioni fondamentali relative alla cybersecurity e alle azioni di attacco e difesa dei sistemi informatici. *Conoscenze e comprensione.* Lo studente acquisirà le conoscenze fondamentali sui concetti teorici e pratici alla base dei Sistemi Operativi, inclusi l'evoluzione storica, la struttura interna, la gestione dei processi, lo scheduling della CPU, la gestione della memoria e la struttura del files system. Inoltre, verranno approfonditi i concetti di base riguardanti la sicurezza informatica, inclusi i principi della triade CIA (Confidenzialità, Integrità, Disponibilità), le principali minacce informatiche e i meccanismi di protezione dei dati. Gli studenti acquisiranno competenze teoriche sui metodi crittografici, sulla gestione delle chiavi digitali e sulle architetture di sicurezza nei contesti cloud. *Capacità di applicare conoscenze e comprensione.* Lo studente svilupperà competenze per essere in grado di configurare ambienti operativi sicuri e funzionali (es. Docker, Nginx), gestire processi e risorse di sistema in ambiente Linux, utilizzare i principali comandi da terminale del SO Linux per automatizzare operazioni, gestire autenticazioni avanzate (MFA, SSO), configurare protocolli sicuri (HTTPS, VPN, SSH) e analizzare scenari reali di attacco e difesa, anche con attività di ethical hacking controllato. *Autonomia di giudizio e pensiero critico:* Al termine del corso lo studente sarà in grado di analizzare criticamente il funzionamento di un sistema operativo, identificare potenziali vulnerabilità, valutare rischi informatici e scegliere soluzioni tecniche adeguate in base al contesto tecnologico e organizzativo. Viene promossa una riflessione autonoma sul bilanciamento tra sicurezza, usabilità e conformità normativa. *Abilità comunicative:* Gli studenti svilupperanno la capacità di documentare e descrivere in modo chiaro e tecnico il funzionamento di un sistema operativo, la gestione dei processi e delle risorse di calcolo, i concetti e le scelte progettuali in termini di sicurezza a interlocutori con diversi livelli di competenza, redigendo report tecnici, documentazione di configurazione e relazioni su casi studio, anche tramite il confronto e la collaborazione nei lavori di gruppo. *Capacità di apprendimento:* Il corso fornisce una base metodologica e strumenti pratici per affrontare l'evoluzione tecnologica dei sistemi operativi e del settore cybersecurity, stimolando

	l'apprendimento autonomo e permanente tramite l'esplorazione di strumenti open source, documentazione tecnica e aggiornamenti sulle vulnerabilità emergenti, grazie anche all'esperienza diretta acquisita nei laboratori pratici.

Programma	Il programma del corso è composto dai seguenti contenuti didattici:
	• Sistemi Operativi
	  ○ Evoluzione, concetti di base e struttura di un SO
	  ○ Processi e CPU scheduling
	  ○ Gestione della memoria e File System
	  ○ Laboratori pratici: SO Linux e la shell Bash
	• Cybersecurity
	  ○ Concetti base di sicurezza: CIA (Confidenzialità, Integrità, Disponibilità)
	  ○ Minacce, vulnerabilità e attacchi
	  ○ Crittografia simmetrica/asimmetrica e algoritmi principali (AES, RSA)
	  ○ Firma digitale, certificati digitali e gestione delle chiavi (PKI)
	  ○ Sicurezza in scenari cloud: protocollo HTTPS/TLS, autenticazione multifattoriale (MFA), Single Sign-On (SSO) e federazione delle identità, VPN, SSH e protocolli sicuri
	  ○ Laboratori pratici e casi di studio: Docker e ambienti virtualizzati, introduzione a Nginx e configurazioni di esempio, esempi di ethical hacking

Tipologie di attività didattiche previste e relative modalità di svolgimento	L'insegnamento è strutturato in lezioni di didattica frontale, incoraggiando l'interazione e la partecipazione attiva degli studenti, ed esercitazioni, integrate con le lezioni e svolte con l'ausilio di un elaboratore. È previsto inoltre l'utilizzo di tecnologie digitali per l'erogazione delle lezioni e delle esercitazioni.
Metodi e criteri di valutazione dell'apprendimento	La valutazione dell'apprendimento (sia per studenti frequentanti che non frequentanti) consiste nello svolgimento di una prova scritta contenente quesiti teorici e pratici relativi ai contenuti del corso, proposti attraverso domande a risposta aperta e/o multipla. A seguito della prova scritta, lo studente potrà richiedere di sostenere una prova orale facoltativa da svolgersi nella data prevista per la visione degli elaborati. In questo caso, la prova scritta concorrerà alla composizione del voto finale, nella misura del 70%. Il restante 30% della valutazione si baserà sul colloquio orale finale. La valutazione del colloquio orale è espressa in trentesimi e terrà conto della proprietà di linguaggio, della capacità argomentativa, di analisi critica e di ragionamento.
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	La valutazione dell'apprendimento prevede l'attribuzione di un voto finale espresso in trentesimi. Il voto finale sarà determinato attraverso l'esame scritto sopra dettagliato. In particolare, il test si compone di 11 quesiti (3 punti per ciascun quesito) per un totale di 33 punti. La concessione della lode sarà valutata per i soli studenti che abbiano raggiunto la valutazione complessiva superiore a 30/30.
Propedeuticità	Non sono richiesti prerequisiti specifici, ma è auspicabile una buona familiarità con l'uso di un elaboratore e aver superato il corso di Fondamenti di Informatica.
Materiale didattico utilizzato e materiale didattico consigliato	– Report, documenti e slides fornite dal docente – I MODERNI SISTEMI OPERATIVI 5/Ed. Andrew S. Tanenbaum, Herbert Bos. Pearson, 2023 (ISBN 9788891931955) – SICUREZZA DEI COMPUTER E DELLE RETI. William Stallings - Giuseppe Lo Re - Alessandra De Paola. Pearson - Ediz. MyLab. 2022 (ISBN: 9788891915290)