Syllabus

Descrizione corso

Titolo insegnamento	Management of System Security and Networks
Codice insegnamento	76437
Titolo aggiuntivo	
Settore Scientifico-Disciplinare	IINF-05/A
Lingua	Italiano
Corso di Studio	Corso di laurea in Informatica e Management delle Aziende digitali
Altri Corsi di Studio (mutuati)	
Docenti	prof. Fabrizio Maria Maggi, maggi@inf.unibz.it https://www.unibz.it/en/faculties/engineering/academic-staff/person/41895
Assistente	
Semestre	Primo semestre
Anno/i di corso	2
CFU	6
Ore didattica frontale	40
Ore di laboratorio	20
Ore di studio individuale	90
Ore di ricevimento previste	18
Sintesi contenuti	- Concetti chiave di sicurezza dei sistemi e dei sistemi in rete, minacce e sicurezza dei dati - Meccanismi di base della crittografia - Sicurezza del software - Sicurezza delle applicazioni Web - Infrastrutture di sicurezza e certificati - Sicurezza della rete - Gestione del rischio
Argomenti	Il corso introduce i concetti fondamentali relativi alla sicurezza dei

dell'insegnamento	sistemi informatici e delle reti, illustrando le principali minacce e le strategie per proteggere dati, applicazioni e infrastrutture. L'insegnamento inizia con una panoramica sui concetti chiave di sicurezza dei sistemi e dei sistemi in rete, evidenziando i principi di confidenzialità, integrità e disponibilità delle informazioni, nonché i concetti di autenticazione, autorizzazione e accountability. Viene inoltre illustrata la varietà di minacce informatiche, inclusi virus, worm, trojan, ransomware e spyware, e come queste possano compromettere la sicurezza dei dati e dei sistemi. Successivamente, il corso approfondisce i meccanismi di base della crittografia. Si spiegano le differenze tra crittografia simmetrica e asimmetrica, le modalità di gestione delle chiavi, e l'uso di firme digitali per garantire autenticità e integrità dei dati. Viene affrontato anche il concetto di hashing, le proprietà delle funzioni hash e le problematiche legate alle collisioni. Inoltre, il corso descrive i metodi per lo scambio sicuro di chiavi e le applicazioni pratiche dei certificati digitali. Un altro focus del corso è la sicurezza delle applicazioni web. Si analizzano le vulnerabilità più comuni, come SQL injection, cross-site scripting (XSS) e cross-site request forgery (CSRF), spiegando come queste possano essere sfruttate dagli attaccanti. Si discute la sicurezza del software, includendo le problematiche legate ai buffer overflow, e si illustrano le principali strategie per prevenire tali vulnerabilità. Il corso tratta le architetture dei dispositivi di sicurezza e le infrastrutture correlate. Vengono descritti firewall, sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS), proxy e altri dispositivi. Si approfondisce il ruolo delle infrastrutture a chiave pubblica (PKI) e dei certificati digitali, fondamentali per garantire autenticità nella comunicazione digitale. Un modulo specifico è dedicato alla sicurezza delle reti, con particolare attenzione ai protocolli di comunicazione sicura, al controllo degli accessi, alla segmentazione della rete e alle tecniche di protezione da intercettazioni. Vengono illustrate le minacce come ARP poisoning, DNS poisoning e attacchi man-in-the-middle, insieme alle contromisure per mitigarle.

	Infine, il corso si concentra sulla gestione del rischio e sulle strategie di resilienza. Vengono trattate la valutazione del rischio, l'analisi delle minacce, la definizione di politiche di sicurezza e piani di mitigazione. Si approfondiscono concetti come ridondanza, fault tolerance, sistemi di backup e disaster recovery.
Parole chiave	Crittografia, Sicurezza delle Applicazioni Web, Sicurezza del Software, Sicurezza delle Reti, Risk Management
Prerequisiti	Gli studenti devono conoscere i concetti di base della programmazione, le strutture dati e gli algoritmi. Questi prerequisiti sono coperti da qualsiasi laurea triennale in Informatics and Management of Digital Business.
Insegnamenti propedeutici	
Modalità di insegnamento	Lezioni frontali in aula e sessioni di laboratorio.
Obbligo di frequenza	La frequenza non è obbligatoria ma consigliata. Gli studenti non frequentanti devono contattare il docente all'inizio del corso per concordare le modalità dello studio indipendente. Le modalità d'esame per gli studenti non frequentanti sono le stesse degli studenti frequentanti.
Obiettivi formativi specifici e risultati di apprendimento attesi	Il corso appartiene alla tipologia "caratterizzante - informatica". L'obiettivo principale di questo esame è fornire un'introduzione al campo della sicurezza informatica. Gli studenti imparano a conoscere l'aspetto tecnico e gestionale della sicurezza nei sistemi informativi. Acquisiscono conoscenze sui principi fondamentali della sicurezza e sugli approcci pratici alla sicurezza dei sistemi informativi. Conoscenza e comprensione: - D1.7 - Conoscere i concetti principali delle reti informatiche e della sicurezza nei sistemi distribuiti. Conoscenza e capacità di comprensione applicate: - D2.3 - Capacità di analizzare problemi aziendali e di sviluppare proposte di soluzione con l'ausilio di strumenti informatici. - D2.4 - Capacità di formalizzare e analizzare procedure e processi operativi, di riconoscere e utilizzare i potenziali di ottimizzazione. - D2.10 - Capacità di gestione di infrastrutture e progetti informatici. Formulare giudizi

	- D3.2 - Essere in grado di lavorare in modo indipendente in base al proprio livello di conoscenza e comprensione, assumendo anche la responsabilità di progetti di sviluppo o di consulenza informatica. Capacità di apprendimento - D5.3 - Capacità di seguire i rapidi sviluppi tecnologici e di conoscere gli aspetti innovativi delle tecnologie e dei sistemi informatici di ultima generazione.
Obiettivi formativi specifici e risultati di apprendimento attesi (ulteriori info.)	
Modalità di esame	- Progetto per verificare le capacità di applicazione delle conoscenze - Esame orale con domande di verifica e discussione del progetto
Criteri di valutazione	Valutazione 1: progetto (30%) Valutazione 2: esame orale (70%) Pertinenti per la valutazione 1: capacità di applicare le conoscenze in un contesto pratico, capacità di riassumere con parole proprie, capacità di spiegare le cose bilanciando concisione e completezza. Pertinente per la valutazione 2: chiarezza delle risposte, capacità di ricordare i principi e i metodi utilizzati nella sicurezza informatica, abilità nell'applicare le conoscenze sulla sicurezza informatica.
Bibliografia obbligatoria	CompTIA Security+ Guide to Network Security Fundamentals 6thEdition, Mark Ciampa ISBN 978-1337288781 Materiale fornito sotto forma di slide e articoli scientifici forniti dal docente.
Bibliografia facoltativa	Computer & Internet Security: A Hands-on Approach 3a Edizione ISBN: 978-17330039-4-0 Computer Security: A Hands-on Approach 3a edizione ISBN: 978-17330039-5-7

	Internet Security: A Hands-on Approach 3a edizione ISBN: 978-17330039-6-4
Altre informazioni	Software utilizzato: Fornito dal docente durante le lezioni/le sessioni di laboratorio.
Obiettivi di Sviluppo Sostenibile (SDGs)	Istruzione di qualità