Syllabus

Descrizione corso

Titolo insegnamento	Network Security
Codice insegnamento	76264
Titolo aggiuntivo	
Settore Scientifico-Disciplinare	
Lingua	Italiano
Corso di Studio	Corso di laurea in Informatica
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 dr. Florian Hofer, Florian.Hofer@unibz.it https://www.unibz.it/en/faculties/engineering/academic-staff/person/37220
Assistente	
Semestre	Primo semestre
Anno/i di corso	3
CFU	12
Ore didattica frontale	80
Ore di laboratorio	40
Ore di studio individuale	180
Ore di ricevimento previste	36
Sintesi contenuti	Modulo 1: Reti informatiche • Introduzione alle reti informatiche • Modello di riferimento ISO/OSI • Applicazioni Internet e protocolli applicativi (HTTP, SMTP, DNS) • Protocolli di rete: TCP/IP, Ethernet • Socket e RPC

	• Resilienza ai guasti, sicurezza Modulo 2: Sicurezza delle informazioni • Definizioni di base: CIA, minaccia, attacco, vulnerabilità, controllo degli accessi • Valutazione dei rischi • Nozioni di base di crittografia • Attacchi e difesa di rete • Usabilità • Politiche di sicurezza
Argomenti dell'insegnamento	Modulo 1: Reti informatiche Il corso si propone di fornire una solida preparazione sulle reti di computer. La teoria sarà intrecciata con discussioni su come le nozioni introdotte vengono sfruttate nella pratica, prendendo come riferimento il framework Java. Questo permetterà di vedere, in contesti reali, perché i sistemi distribuiti sono importanti. Modulo 2: Sicurezza delle informazioni Il corso introduce i concetti fondamentali relativi alla sicurezza dei 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 descrive nel dettaglio il ruolo dei

	cookies nel contesto della sicurezza delle applicazioni Web. 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	Modulo 1: Reti informatiche Internet, TCP/IP, Reti, Protocolli Modulo 2: Sicurezza delle informazioni Crittografia, Sicurezza delle Applicazioni Web, Sicurezza del Software, Sicurezza delle Reti, Risk Management
Prerequisiti	Modulo 1: Reti informatiche Il corso richiede una conoscenza di base delle strutture dati e degli algoritmi, oltre a competenze fondamentali in Java. Modulo 2: Sicurezza delle informazioni Gli studenti devono conoscere i concetti di base della programmazione, le strutture dati e gli algoritmi.
Insegnamenti propedeutici	
Modalità di insegnamento	Modulo 1: Reti informatiche Il corso prevede lezioni frontali ed esercitazioni di laboratorio. Modulo 2: Sicurezza delle informazioni Lezioni frontali in aula e sessioni di laboratorio.

Obbligo di frequenza	La frequenza non è obbligatoria, ma è vivamente consigliata. Gli studenti che non intendono frequentare il corso sono pregati di contattare il docente all'inizio del corso per concordare le modalità dello studio autonomo.
Obiettivi formativi specifici e risultati di apprendimento attesi	Conoscenze e comprensione - D1.11 Conoscere approfonditamente i principali concetti di reti informatiche e di sistemi distribuiti (attività nei settori scientifici disciplinari INF/01 e ING-INF/05) - D.12 Conoscere approfonditamente i fondamenti di sistemi Internet e le metodologie per il loro sviluppo e progettazione (attività nei settori scientifici disciplinari INF/01 e ING-INF/05) - D1.14 Conoscere le criticità di sicurezza dei sistemi informatici, i concetti di base di sicurezza e le tecniche di sviluppo di sistemi sicuri (attività nei settori scientifici disciplinari INF/01 e ING-INF/05) Applicazione delle conoscenze e della comprensione - D2.09 Capacità di progettare e programmare in ambienti informatici distribuiti e su reti informatiche. - D2.11 Capacità di analizzare la qualità di un sistema informatico e identificarne gli aspetti critici (attività nei settori scientifici disciplinari INF/01 e ING-INF/05) - D2.17 Capacità di analizzare e migliorare gli aspetti di privatezza e sicurezza dei dati nel contesto di complesse infrastrutture software (attività nei settori scientifici disciplinari INF/01 e ING-INF/05) - D2.19 Saper applicare la propria conoscenza in diversi contesti lavorativi (attività nei settori scientifici disciplinari SECS-P/07, ING-INF/01, INF/01 e ING-INF/05) Capacità di giudizio: - D3.1 Capacità di raccogliere ed interpretare dati utili per formare giudizi autonomi su sistemi informativi ed il loro utilizzo. - D3.2 Essere in grado di lavorare in autonomia adeguata al proprio livello di conoscenza e comprensione. Capacità di comunicazione: - D4.1 Essere in grado di utilizzare una delle tre lingue: inglese, italiano e tedesco, e essere in grado di utilizzare terminologia tecnica e comunicativa appropriata.

	- D4.2 Capacità di utilizzare i più moderni strumenti di comunicazione anche a distanza. - D4.5 Capacità di collaborare in gruppi di lavoro per la realizzazione di sistemi informatici. Capacità di apprendimento: - D5.1: Capacità di apprendimento necessarie per intraprendere studi successivi con alto grado di autonomia. - D5.3: Capacità di seguire la rapida evoluzione tecnologica e di apprendere gli aspetti innovativi di tecnologie e sistemi informatici di ultima generazione.
Obiettivi formativi specifici e risultati di apprendimento attesi (ulteriori info.)	
Modalità di esame	Modulo 1: Reti informatiche La valutazione consiste in un esame orale (D1.11, D1.12, D4.1, D5.1, D5.3) e in relazioni di laboratorio, di cui esercizi pratici (D1.11, D1.12, D2.9, D4.1, D4.2) e compiti a progetto (D2.9, D3.1, D3.2, D4.2, D5.1). Modulo 2: Sicurezza delle informazioni - Progetto per verificare le capacità di applicazione delle conoscenze - Esame orale con domande di verifica e discussione del progetto
Criteri di valutazione	Modulo 1: Reti informatiche Il voto finale è calcolato come media ponderata delle relazioni di laboratorio (30%) e dell'esame orale (70%). Tuttavia, i voti delle relazioni di laboratorio vengono considerati solo se sono superiori al voto dell'esame orale. Il peso del 30% per le relazioni di laboratorio si applica solo se vengono consegnati tre compiti; se vengono consegnati meno compiti, il peso viene modificato in proporzione. Modulo 2: Sicurezza delle informazioni Valutazione 1: progetto (30%) Valutazione 2: esame orale (70%) Il completamento del progetto con un voto sufficiente è propedeutico all'esame orale dato che l'esame orale parte da una

	discussione del progetto. 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	Modulo 1: Reti informatiche James Kurose e Keith Ross. Computer Networking: A Top-Down Approach. Pearson, Boston Munich, 7ª edizione, aprile 2016. ISBN 978-0-13-359414-0. Modulo 2: Sicurezza delle informazioni 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	Modulo 1: Reti informatiche Andrew Tanenbaum e David Wetherall. Reti di computer. Pearson, Boston, 5a edizione, settembre 2010. ISBN 978-0-13-212695-3. Andrew S. Tanenbaum e Maarten van Steen. Sistemi distribuiti: Principles and Paradigms. CreateSpace Independent Publishing Platform, Paesi Bassi, 2a edizione, febbraio 2016. ISBN 978-1-5302-8175-6 Modulo 2: Sicurezza delle informazioni

	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
Altre informazioni	Modulo 1: Reti informatiche Software utilizzato: Wireshark (https://www.wireshark.org) Java (https://openjdk.org) *nix tools (*sh, *ssh, iproute2, dig, tracepath..) Modulo 2: Sicurezza delle informazioni Software utilizzato: Fornito dal docente durante le lezioni/le sessioni di laboratorio.
Obiettivi di Sviluppo Sostenibile (SDGs)	Istruzione di qualità

Modulo del corso

Titolo della parte costituente del corso	Computer Networks
Codice insegnamento	76264A
Settore Scientifico-Disciplinare	IINF-05/A
Lingua	Italiano
Docenti	dr. Florian Hofer, Florian.Hofer@unibz.it https://www.unibz.it/en/faculties/engineering/academic-staff/person/37220
Assistente	
Semestre	Primo semestre
CFU	6
Docente responsabile	
Ore didattica frontale	40
Ore di laboratorio	20

Ore di studio individuale	90
Ore di ricevimento previste	18
Sintesi contenuti	• Introduzione alle reti informatiche • Modello di riferimento ISO/OSI • Applicazioni Internet e protocolli applicativi (HTTP, SMTP, DNS) • Protocolli di rete: TCP/IP, Ethernet • Socket e RPC • Resilienza ai guasti, sicurezza
Argomenti dell'insegnamento	Il corso si propone di fornire una solida preparazione sulle reti di computer. La teoria sarà intrecciata con discussioni su come le nozioni introdotte vengono sfruttate nella pratica, prendendo come riferimento il framework Java. Questo permetterà di vedere in contesti reali perché i sistemi distribuiti sono importanti.
Modalità di insegnamento	Il corso prevede lezioni frontali ed esercitazioni di laboratorio. Software utilizzato: Wireshark (https://www.wireshark.org) Java (https://openjdk.org) *nix tools (*sh, *ssh, iproute2, dig, tracepath..)
Bibliografia obbligatoria	James Kurose e Keith Ross. Computer Networking: A Top-Down Approach. Pearson, Boston Munich, 7ª edizione, aprile 2016. ISBN 978-0-13-359414-0.
Bibliografia facoltativa	Andrew S. Tanenbaum e Maarten van Steen. Sistemi distribuiti: Principles and Paradigms. CreateSpace Independent Publishing Platform, Paesi Bassi, 2a edizione, febbraio 2016. ISBN 978-1-5302-8175-6

Modulo del corso

Titolo della parte costituente del corso	Information Security
Codice insegnamento	76264B
Settore Scientifico-Disciplinare	IINF-05/A
Lingua	Italiano
Docenti	prof. Fabrizio Maria Maggi, maggi@inf.unibz.it https://www.unibz.it/en/faculties/engineering/academic-

	staff/person/41895
Assistente	
Semestre	Primo semestre
CFU	6
Docente responsabile	
Ore didattica frontale	40
Ore di laboratorio	20
Ore di studio individuale	90
Ore di ricevimento previste	18
Sintesi contenuti	• Definizioni di base: CIA, minaccia, attacco, vulnerabilità, controllo degli accessi • Valutazione dei rischi • Nozioni di base di crittografia • Attacchi e difesa di rete • Usabilità • Politiche di sicurezza
Argomenti dell'insegnamento	Il corso introduce i concetti fondamentali relativi alla sicurezza dei 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.
Modalità di insegnamento	Lezioni frontali e Laboratori
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