Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	**Sicurezza nelle Reti e nei Sistemi Distribuiti**	
Corso di studio	Laurea Magistrale in Sicurezza Informatica	
Anno Accademico	2023/24	
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)		6 CFU
Settore Scientifico Disciplinare	INF/01	
Lingua di erogazione	Italiano	
Anno di corso	Primo	
Periodo di erogazione	2^semestre, le date esatte sono riportate nel manifesto/regolamento	
Obbligo di frequenza	La frequenza è fortemente raccomandata	
Sito web del corso di studio	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica	

Docente/i

Nome e cognome	Fabio Calefato
Indirizzo mail	fabio.calefato@uniba.it
Telefono	usare Microsoft Teams
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n.665, 6^ piano.
Sede virtuale	Piattaforma ADA - https://elearning.di.uniba.it/
Sito web del docente	https://collab.di.uniba.it/fabio
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Venerdì 11-12 previa richiesta di appuntamento

Syllabus

Obiettivi formativi	Lo studente apprenderà i concetti fondamentali della sicurezza delle reti di calcolatori e nei sistemi distribuiti, con particolare riferimento ai livelli applicativi della pila di protocolli TPC/IP.

Prerequisiti	*Le seguenti conoscenze preliminari facilitano ed accelerano la comprensione degli argomenti dell'insegnamento:* ● *conoscenza dei principali protocolli di rete Internet.*
Contenuti di insegnamento (Programma)	• Parte I: Fondamenti di crittografia applicata alla sicurezza delle reti ○ Riservatezza della comunicazione tramite cifratura simmetrica ○ Principi di cifratura simmetrica ○ Cifrari a blocchi e a flusso ○ Generatori di numeri casuali e pseudocasuali ○ Riservatezza della comunicazione tramite cifratura asimmetrica ○ Approcci all'autenticazione dei messaggi ○ Funzioni hash sicure e MAC ○ Principi di cifratura asimmetrica ○ Firma digitale • Parte II: Sicurezza nei protocolli di rete ○ Protocolli di distribuzione delle chiavi e autenticazione utente ○ Distribuzioni di chiave di cifratura tramite cifratura simmetrica ○ Cenni su Kerberos ○ Distribuzioni di chiavi tramite cifratura asimmetrica ○ Cenni su X.509 ○ Lo stack TCP/IP ○ Architettura dell'e-mail ○ Sicurezza nella posta elettronica: S/MIME e PGP ○ Sicurezza a livello di trasporto: HTTPS e SSH ○ Sicurezza a livello IP: IPSec ○ Internet Key Exchange ○ Cenni su sicurezza delle reti Wi-Fi • Parte III: Sicurezza dei sistemi ○ Malware e classificazione dei malicious software ○ Intrusion detection systems ○ Firewall
Testi di riferimento	Per i contenuti relativi alla sicurezza delle reti e dei sistemi: William Stallings, Network Security Essentials: Applications and Standards (6th Edition), Pearson. Per la parte relativa alla descrizione dei protocolli di rete e dello stack TCP/IP: J.F. Kurose & K.W. Ross, Reti di calcolatori e Internet - Un approccio top-down (8 edizione), Pearson.
Note ai testi di riferimento	I libri di testo sono integrati con gli appunti presi a lezione e con le slide del docente disponibili sulla piattaforma di e-learning Ada.

Organizzazione della didattica

Ore

Totali	Didattica frontale	Pratica (laboratorio, progetto, esercitazione, altro)	Studio individuale
150 ore	32 ore	30 ore	88 ore

CFU/ETCS

6 CFU	4 CFU	2 CFU	

Metodi didattici	
	Lezioni frontali supportate da slide ed esercitazioni in aula.

Risultati di apprendimento previsti	
Conoscenza e capacità di comprensione	● *Conoscenza e capacità di comprensione* ○ Conoscere i concetti di base della sicurezza di rete. ○ Conoscere i fondamenti di crittografia applicati alla sicurezza in rete ○ Conoscere le principali forme di attacco alla sicurezza delle reti ○ Conoscere le principali forme di difesa dagli attacchi alla sicurezza delle reti
Conoscenza e capacità di comprensione applicate	● *Conoscenza e capacità di comprensione applicate* ○ Acquisire familiarità con la prevenzione di attacchi che compromettano la disponibilità, l'integrità e la riservatezza delle informazioni scambiate in rete.
Competenze trasversali	**Autonomia di giudizio** Mostrare di aver acquisito autonomia di giudizio sulle scelte relative alla sicurezza nel funzionamento delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti. **Abilità comunicative** Mostrare di essere in grado di comunicare in modo appropriato le caratteristiche e le specifiche tecniche relativamente alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti. **Capacità di apprendere in modo autonomo** Mostrare di aver sviluppato capacità di intraprendere in autonomia ulteriori approfondimenti su argomenti attinenti alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti.

Valutazione	
Modalità di verifica dell'apprendimento	L'esame si svolge mediante prova scritta (voto in trentesimi). Tale prova nel rispondere a un questionario contenente domande a risposta chiusa o aperta e brevi esercizi.
Criteri di valutazione	● **Conoscenza e capacità di comprensione:** Lo studente dovrà dimostrare di conoscere e di aver compreso i concetti fondamentali attinenti alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti. ● **Conoscenza e capacità di comprensione applicate:** Lo studente dovrà dimostrare di saper applicare i concetti fondamentali attinenti alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti, al fine di evitare e prevenire minacce alla riservatezza, disponibilità, e integrità delle informazioni ivi scambiate. ● **Autonomia di giudizio:**

	○ Lo studente dovrà dimostrare di saper formulare un proprio giudizio sulle scelte relative alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti ● **Abilità comunicative:** Lo studente dovrà dimostrare di saper comunicare le conoscenze acquisite nonché motivare le proprie scelte implementative in modo appropriato, con riferimento alle caratteristiche tecniche attinenti alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti. ● **Capacità di apprendere:** Lo studente dovrà dimostrare di aver acquisito la capacità di approfondire in autonomia gli argomenti attinenti alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti.
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	I risultati di apprendimento previsti saranno misurati mediante prova scritta è valutata in trentesimi.
Altro	Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti: ● https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea ● https://www.uniba.it/it/ricerca/dipartimenti/informatica ● https://elearning.di.uniba.it/ I programmi degli insegnamenti sono disponibili qui: ● https://programmi.di.uniba.it/ Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei Regolamenti didattici e manifesti degli studi disponibili nel sito: ● https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento. _____ Il link al corso sulla piattaforma e-learning del dipartimento ADA: ● https://elearning.di.uniba.it/course/view.php?id=2067