PROGRAMMA DEL CORSO DI SICUREZZA DEI SISTEMI INFORMATICI

SETTORE SCIENTIFICO

ING-INF/05 (IINF-05/A)

CFU

9

ATTIVITÀ DIDATTICA EROGATIVA (DE)

Le attività di Didattica Erogativa consistono, per ciascun CFU, nell erogazione di 5 videolezioni della durata di circa 30 minuti. A ciascuna lezione sono associati: • una dispensa (PDF) di supporto alla videolezione oppure l'indicazione di capitoli o paragrafi di un ebook di riferimento, scelto dal docente tra quelli liberamente consultabili in piattaforma da studentesse e studenti; • un questionario a risposta multipla per l'autoverifica dell'apprendimento.

TESTO CONSIGLIATO

"Crittografia e Sicurezza delle Reti" 2 ed., William Stallings, Ed. McGraw-Hill "Computer Security: Principles and Practice" 4 ed., Stallings W., Brown L., Pearson Education Limited

MODALITÀ DI VERIFICA DELL'APPRENDIMENTO

L'esame può essere sostenuto sia in forma scritta che in forma orale. L'esame orale consiste in un colloquio con la Commissione sui contenuti dell'insegnamento. L'esame in forma scritta consiste nello svolgimento di un test composto da 31 domande. Per ogni domanda lo studente deve scegliere una delle 4 possibili risposte. Solo una risposta è corretta e, in caso di risposte errate o mancanti, non sarà attribuita alcuna penalità. Rispondendo correttamente a tutte le 31 domande, si conseguirà la lode. Oltre alla prova d'esame finale, il percorso prevede attività di didattica interattiva sincrona e prove intermedie che consentono alle studentesse e agli studenti di monitorare il proprio apprendimento, attraverso momenti di verifica progressiva e consolidamento delle conoscenze. La partecipazione alle attività di didattica interattiva sincrona consente di maturare una premialità fino a 2 punti sul voto finale, attribuiti in funzione della qualità della partecipazione alle attività e dell'esito delle prove. Per accedere alle prove intermedie è necessario aver seguito almeno il 50% di ogni ora di didattica interattiva. Le prove intermedie possono consistere in un test di fine lezione o nella predisposizione di un elaborato. Le prove intermedie si considerano superate avendo risposto correttamente ad almeno l'80% delle domande di fine lezione. In caso di prove intermedie che prevedano la redazione di un elaborato, il superamento delle stesse ai fini della premialità sarà giudicata dal docente titolare dell'insegnamento. I punti di premialità, previsti per le prove intermedie, sono sommati al voto finale d'esame solo se la prova d'esame è superata con un punteggio pari ad almeno 18/30 e possono contribuire al conseguimento della lode. Le modalità d'esame descritte sono progettate per valutare il grado di comprensione delle nozioni teoriche e la capacità di applicazione delle stesse e consentiranno di valutare il livello di competenza e l'autonomia di giudizio

maturati dalla studentessa e dallo studente. Le abilità di comunicazione e la capacità di apprendimento saranno valutate anche attraverso le interazioni dirette che avranno luogo durante la fruizione dell'insegnamento. Le studentesse e gli studenti hanno la facoltà di utilizzare calcolatrici, fogli bianchi o ulteriori ausili per l'espletamento delle prove.

RECAPITI

leonardo.galteri@unipegaso.it valerio.deluca@unipegaso.it salvatore.barone@unipegaso.it andrea.generosi@unipegaso.it

OBBLIGO DI FREQUENZA

A studentesse e studenti viene richiesto di partecipare ad almeno il 70% delle attività di didattica erogativa. Per l'accesso alla prova d'esame è, inoltre, necessaria la redazione di un elaborato giudicato sufficiente dal docente titolare dell'insegnamento".

AGENDA

/**/
Nella sezione Informazioni Appelli, nella home del corso, per ogni anno accademico vengono fornite le date degli appelli d'esame. Le attività di didattica interattiva sincrona sono calendarizzate in piattaforma nella sezione Class. Le attività di ricevimento di studenti e studentesse sono calendarizzate nella sezione Ricevimento Online.

OBIETTIVI FORMATIVI PER IL RAGGIUNGIMENTO DEI RISULTATI DI APPRENDIMENTO PREVISTI NELLA SCHEDA SUA

L'obiettivo del corso è sviluppare le competenze tecniche, teoriche e applicative necessarie per comprendere e gestire efficacemente la sicurezza nelle tecnologie dell'informazione e delle comunicazioni. Obiettivi formativi: 1. Fornire una solida comprensione dei concetti di base di sicurezza, dei servizi e dei meccanismi di sicurezza per permettere agli studenti di identificare e analizzare le vulnerabilità e le minacce alla sicurezza. 2. Dotare gli studenti di una conoscenza approfondita delle tecniche di crittografia, sia simmetrica che asimmetrica, incluse le tecniche di sostituzione, trasposizione, cifratura a blocchi e gli standard come DES, AES, RSA, tra gli altri. Gli studenti dovrebbero essere capaci di applicare questi metodi per garantire la confidenzialità, l'integrità e l'autenticazione delle informazioni. 3. Insegnare metodi efficaci per la gestione delle chiavi e per la sicurezza nell'ambito delle comunicazioni e delle transazioni, includendo l'uso di certificati, firme digitali, e protocolli come IPSec e SSL/TLS. 4. Formare gli studenti sulla sicurezza delle applicazioni, dei sistemi operativi, dei database e del cloud, nonché sulle misure preventive come antivirus e firewall, e sistemi di rilevazione delle intrusioni. 5. Aggiornare gli studenti sulle ultime tendenze e innovazioni in sicurezza, come la blockchain, la sicurezza IoT e le comunicazioni anonime, per prepararli a fronteggiare le sfide emergenti nel campo della sicurezza.

RISULTATI DI APPRENDIMENTO ATTESI

- Conoscenza e capacità di comprensione Capacità di definire strategie progettuali, operative e gestionali, necessarie a garantire un livello di sicurezza adeguato nei luoghi di lavoro, sia dal punto di vista della safety che della security, in ambito sia civile che industriale - Capacità di applicare conoscenza e comprensione Capacità di applicare le conoscenze per realizzare e/o verificare progetti e/o interventi in materia di sicurezza e impatto ambientale relativi a impianti, strutture, infrastrutture e processi al fine di garantire un idoneo livello di sicurezza delle persone e dell'ambiente; Capacità di applicare la comprensione delle situazioni di rischio legate agli impianti civili e industriali e alle infrastrutture, sviluppando soluzioni tecniche per prevenire danni e mettere in sicurezza infrastrutture e impianti. Capacità di applicare la comprensione di processi complessi e di proporre strategie di reingegnerizzazione atte a favorire un'ottimizzazione degli stessi. - Autonomia di giudizio Capacità di analisi delle complessità per la mitigazione dei rischi e una riformulazione sostenibile di processi e sistemi Capacità di integrare conoscenze tecniche, ambientali e gestionali per prendere decisioni autonome in contesti complessi. - Abilità comunicative Capacità di dialogare efficacemente con professionisti di diversi settori, esprimendo concetti tecnici con precisione e adattando il linguaggio al livello di competenza dell'interlocutore. Capacità di presentare analisi e redigere rapporti tecnici in modo accurato per garantire una corretta comprensione e utilizzo delle informazioni. Capacità di integrare efficacemente le diverse forme di comunicazione nelle fasi di progettazione, esercizio e monitoraggio, assicurando il coordinamento tra tutte le parti coinvolte. - Capacità di apprendere Capacità di acquisire nuove strategie per ottimizzare i processi in un'ottica di sicurezza e sostenibilità.

PREREQUISITI

/**/
Nessuno

PROGRAMMA DIDATTICO: ELENCO VIDEOLEZIONI/MODULI

FONDAMENTI DI SICUREZZA INFORMATICA 1. Concetti base di sicurezza 2. Servizi e meccanismi di sicurezza

CRITTOGRAFIA 3. Crittografia simmetrica 4. Cifratura a blocchi 5. La crittografia multipla 6. Segretezza e crittografia simmetrica 7. Crittografia asimmetrica 8. L'algoritmo RSA 9. Gestione delle chiavi e scambio Diffie-Hellman

AUTENTICAZIONE E INTEGRITÀ DEI MESSAGGI 10. Autenticazione dei messaggi 11. Codici MAC e funzioni hash 12. L'algoritmo SHA-512 13. Gli algoritmi HMAC e CMAC 14. Le firme digitali

AUTENTICAZIONE UTENTE E CONTROLLO DEGLI ACCESSI 15. Principi di autenticazione utente 16. Autenticazione con password 17. Autenticazione con Token, Biometrica e remota

18. Principio di Controllo degli Accessi 19. Controllo degli Accessi Discrezionale 20. Controllo degli Accessi Basato sui Ruoli 21. Controllo degli Accessi Basato sugli Attributi

SICUREZZA DI RETE 22. ICAM e Trust Frameworks 23. IPSec e il protocollo ESP 24. Sicurezza della posta elettronica e PGP 25. Il protocollo SSL 26. I protocolli TLS e HTTPS

MALWARE E ATTACCHI INFORMATICI 27. Crimini Informatici 28. Malware 29. Virus 30. Worm 31. Trojan, Backdoor, Rootkits 32. Attacchi DoS 33. Buffer Overflow

SICUREZZA DELLE APPLICAZIONI E DELLE INFRASTRUTTURE 34. Sicurezza del Database 35. Sicurezza del Software 36. Sicurezza del Sistema Operativo 37. Sicurezza del Cloud 38. Sicurezza IoT 39. Sicurezza Wireless DIFESE

INFORMATICHE 40. Anti-Virus 41. I firewall 42. Intrusion Detection System

APPROFONDIMENTI 43. Multimedia forensics 44. Comunicazioni anonime: Tor e Deep Web 45. Machine Learning per la sicurezza

ATTIVITÀ DI DIDATTICA INTERATTIVA (DI)

Le attività di Didattica Interattiva (TEL-DI) consistono, per ciascun CFU, in 2 ore erogate in modalità sincrona su piattaforma Class, svolte dal docente anche con il supporto del tutor disciplinare, e dedicate a una o più tra le seguenti tipologie di attività: • sessioni live, in cui il docente guida attività applicative, stimolando la riflessione critica e il confronto diretto con gli studenti tramite domande in tempo reale e discussioni collaborative; • webinar interattivi, arricchiti da sondaggi e domande dal vivo, per favorire il coinvolgimento attivo e la costruzione della conoscenza; • lavori di gruppo e discussioni in tempo reale, organizzati attraverso strumenti collaborativi come le breakout rooms, per sviluppare strategie di problem solving e il lavoro in team; • laboratori virtuali collettivi, in cui il docente guida esperimenti, attività pratiche o l'analisi di casi di studio, rendendo l'apprendimento un'esperienza concreta e partecipativa; Tali attività potranno essere eventualmente supportate da strumenti asincroni di interazione come per esempio: • forum; • wiki; • quiz; • glossario. Si prevede l'organizzazione di almeno due edizioni di didattica interattiva sincrona nel corso dell'anno accademico. Si precisa che il ricevimento degli studenti, anche per le tesi di laurea, non rientra nel computo della didattica interattiva.