PROGRAMMA DEL CORSO DI SICUREZZA DEI SISTEMI INFORMATICI

SETTORE SCIENTIFICO

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

CFU

12

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. Crittografia simmetrica: tecniche di sostituzione e di trasposizione

5. Cifratura a blocchi

6. La cifratura DES: Data Encryption Standard

7. La cifratura AES - Advanced Encryption Standard

8. La crittografia multipla

9. Modalità di funzionamento della cifratura a blocchi

10. Segretezza e crittografia simmetrica

11. Crittografia asimmetrica

12. L’algoritmo RSA

13. Gestione delle chiavi e scambio Diffie-Hellman

AUTENTICAZIONE E INTEGRITÀ DEI MESSAGGI

14. Autenticazione dei messaggi

15. Codici MAC e funzioni hash

16. L’algoritmo SHA-512

17. Gli algoritmi HMAC e CMAC

18. Le firme digitali

19. Autenticazione in ambienti distribuiti

20. I certificati X.509

AUTENTICAZIONE UTENTE E CONTROLLO DEGLI ACCESSI

21. Principi di autenticazione utente

22. Autenticazione con password

23. Autenticazione con Token, Biometrica e remota

24. Principio di Controllo degli Accessi

25. Controllo degli Accessi Discrezionale

26. Controllo degli Accessi Basato sui Ruoli

27. Controllo degli Accessi Basato sugli Attributi

SICUREZZA DI RETE

28. ICAM e Trust Frameworks

29. IPSec e il protocollo ESP

30. Sicurezza della posta elettronica e PGP

31. IPSec

32. Il protocollo SSL

33. I protocolli TLS e HTTPS

34. SET - Secure Electronic Transaction

MALWARE E ATTACCHI INFORMATICI

35. Crimini Informatici

36. Malware

37. Virus

38. Worm

39. Trojan, Backdoor, Rootkits

40. Attacchi DoS

41. Tipologie di DoS

42. Buffer Overflow

SICUREZZA DELLE APPLICAZIONI E DELLE INFRASTRUTTURE

43. Sicurezza del Database

44. Sicurezza del Software

45. Sicurezza del Sistema Operativo

46. Sicurezza del Cloud

47. Sicurezza IoT

48. Sicurezza Wireless

DIFESE INFORMATICHE

49. Anti-Virus

50. I firewall

51. Intrusion Detection System

MULTIMEDIA FORENSIC

52. Multimedia forensics

53. MM-forensics: identificazione della sorgente

54. MM-forensics: rilevazione di fake

BLOCKCHAIN E COMUNICAZIONI ANONIME

55. Blockchain e Proof-of-Work

56. Blockchain e il Ledger Distribuito

57. Comunicazioni anonime: i protocolli Crowds e Mix

58. Comunicazioni anonime: Tor e Deep Web

SICUREZZA AVANZATA E FUTURA

59. Protezione contro Advanced Persistent Threats

60. Security Information and Event Management

61. Tecniche Avanzate di Intrusion Prevention Systems

62. Gestione Avanzata delle Identità e degli Accessi

63. Zero Trust Architecture

64. Sicurezza delle Comunicazioni Satellitari

65. Quantum Key Distribution

66. Sicurezza dei Big Data

67. Forensics in Ambienti Cloud e Virtualizzati

68. Tecniche forensic avanzate

69. AI in Cybersecurity

70. Advanced Endpoint Protection

71. Governance, Risk Management, and Compliance

72. Tecnologie emergenti e privacy

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 comprendere le verifiche di sicurezza in ambito civile, informatico e industriale, con riguardo sia al personale impiegato, che a soggetti esterni, che all'ambiente.

Capacità di identificare i fattori di rischio per la valutazione delle condizioni di sicurezza di progetti, impianti, strutture e processi.

Conoscenza di tecniche avanzate di gestione delle chiavi e protocolli di sicurezza per le comunicazioni.

Capacità di identificare dispositivi e strategie atti alla mitigazione dei rischi.

Conoscenza delle strategie progettuali, operative e gestionali, necessarie a garantire un livello di sicurezza adeguato nei luoghi di lavoro, in ambito sia civile che industriale.

Conoscenza delle tecniche di progettazione e gestione di impianti e sistemi di sicurezza, dal punto di vista sia della safety, che della security, sia in ambito civile che industriale

- Capacità di applicare conoscenza e comprensione

Capacità di realizzare e verificare elaborati progettuali in materia di sicurezza di impianti, strutture e processi al fine di garantire un adeguato livello di sicurezza delle persone e dell'ambiente.

Capacità di valutare le condizioni di sicurezza nei luoghi di lavoro, di servizi e di infrastrutture civili ed industriali.

Capacità di progettare e gestire impianti e sistemi di sicurezza, sia in termini di safety, che di security, relativi a strutture, impianti e processi in ambito sia civile che industriale.

Capacità di valutare l'efficacia di dispositivi e strategie atti alla mitigazione del rischio.

- Autonomia di giudizio

Autonomia di giudizio nella valutazione dell'efficacia di dispositivi e strategie atte alla mitigazione del

rischio.

- Abilità comunicative

Richiedere in modo chiaro e sintetico, ai propri clienti e/o interlocutori, specialisti e non, tutte le informazioni necessarie per risolvere una specifica problematica.

Trasferire in modo chiaro e sintetico, ai propri clienti e/o interlocutori, specialisti e non, tutte le informazioni, dati e risultati richiesti.

- Capacità di apprendere

Capacità di aggiornarsi sui continui sviluppi nell'ambito della sicurezza di carattere tecnico-scientifico riguardo a tecniche, metodologie e strumenti per l'analisi dei rischi.

Capacità di aggiornarsi sui continui sviluppi nell'ambito della sicurezza di carattere tecnico-scientifico riguardo alle tecniche atte a garantire la sicurezza di impianti, strutture e processi.

PREREQUISITI

/**/
Nessuno

ATTIVITÀ DI DIDATTICA INTERATTIVA (DI)

/**/
Le attività di Didattica interattiva consistono, per ciascun CFU, in un'ora dedicata a una o più tra le seguenti tipologie di attività:

- Redazione di un elaborato
- Partecipazione a una web conference
- Partecipazione al forum tematico
- Lettura area FAQ
- Svolgimento delle prove in itinere con feedback

Per gli aggiornamenti, la calendarizzazione delle attività e le modalità di partecipazione si rimanda alla piattaforma didattica dell'insegnamento.

ATTIVITÀ DIDATTICA EROGATIVA (DE)

/**/
Le attività di didattica erogativa consistono, per ciascun CFU, nell'erogazione di 6 videolezioni corredate di testo e questionario finale.

- Il format di ciascuna videolezione prevede il video registrato del docente che illustra le slide costruite con parole chiave e schemi esemplificativi.
- Il materiale testuale allegato a ciascuna lezione corrisponde a una dispensa (PDF) composta da almeno 10 pagine con le informazioni necessarie per la corretta e proficua acquisizione dei contenuti trattati durante la lezione.

Attività di autoverifica degli apprendimenti prevista al termine di ogni singola videolezione consiste in un questionario costituito da 10 domande, a risposta multipla

TESTO CONSIGLIATO

/**/
Gli studenti che intendono approfondire le tematiche del corso, integrando le dispense e i materiali forniti dal docente, possono consultare i seguenti volumi:

- "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.

Gli appelli orali sono previsti nella sola sede centrale. L’esame orale consiste in un colloquio con la Commissione sui contenuti del corso.

L’esame scritto consiste nello svolgimento di un test con 30 domande. Per ogni domanda lo studente deve scegliere una di 4 possibili risposte. Solo una risposta è corretta.

Sia le domande orali che le domande scritte sono formulate per valutare il grado di comprensione delle nozioni teoriche e la capacità di ragionare utilizzando tali nozioni. Le domande sulle nozioni teoriche consentiranno di valutare il livello di comprensione. Le domande che richiedono l’elaborazione di un ragionamento consentiranno di valutare il livello di competenza e l’autonomia di giudizio maturati dallo studente.

Le abilità di comunicazione e la capacità di apprendimento saranno valutate anche attraverso le interazioni dirette tra docente e studente che avranno luogo durante la fruizione del corso (videoconferenze ed elaborati proposti dal docente).

RECAPITI

/**/
leonardo.galteri@unipegaso.it

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

OBBLIGO DI FREQUENZA

/**/

Obbligatoria online. Ai corsisti viene richiesto di visionare almeno l'80% delle videolezioni presenti in piattaforma.

Per accedere all’esame vige l’obbligo di superamento dell’elaborato

AGENDA

In Informazioni Appelli nella home del corso per ogni anno accademico vengono fornite le date degli appelli