PROGRAMMA DEL CORSO DI SICUREZZA DEI SISTEMI INFORMATICI

SETTORE SCIENTIFICO

ING-INF/05

CFU

12

OBIETTIVI

/**/

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.

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