Tématerületek

1. Alapfogalmak: A biztonság megközelítése
2. Adatvédelem és adatbiztonság, Veszélyek, támadások, vírusok, emberi tényező
3. Adatvesztés és helyreállítás
4. Felhasználó hitelesítési módszerek, jelszavak, titkosítás.
5. A magánélet védelme, az adatok megsemmisítése
6. Hálózatbiztonsági ismeretek: protokollok, eszközök, hálózati támadások
7. Virtuális magánhálózatok
8. Etikus hackelés
9. Biztonságos alkalmazások tervezése és megvalósítása

Schedule

Week #	Lecture	Labor
Week 1	Basic concepts	Labor usage, handouts requirements
Week 2	Security design principles	Functional and architectural design of coding task 1.
Week 3	Security design walkthrough	Functional and architectural design of coding task 2.
Week 4	Introduction to Kali Linux	Basic commands
Week 5	Working with Kali Linux	Coding - safe logon and user management
Week 6	Python security tools	Coding - safe document storage
Week 8	Bank Holiday	Bank Holiday
Week 9	Malicious code	Virus and malwae checking tools
Week 10	Cryptography	Kali password storing functions
Week 11	Security coding walkthrough	Coding task pre-evaluation
Week 12	Test	coding task pre-evaluation
Week 13	Presentations of coding assignments	Presentations of coding assignments
Week 14	Evaluation	Presentations of coding assignments

Textbooks

- Stallings, W., Brown, L. (2015): Computer security: principles and practice 3rd edition, Pearson Education, 978-0-13-377392-7
- Matt Bishop (2019): Computer Security Art and Science, Pearson Education 978-0-321-71233-2
- Alan G. Konheim: Computer Security and Cryptography (Wiley, 2007, ISBN: 978-0-471-94783-7)
- John R. Vacca: Computer and Information Security handbook (Morgan Kaufmann, 2009, 844 pages, ISBN 978-0-12-374354-1)
- Simon Singh: The code book ISBN 0385495323
- James M. Stewart, Mike Chapple, Darril Gibson - CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, 2015, ISBN 1119042712
- Tony Hsiang-Chih Hsu - Practical Security Automation and Testing: Tools and techniques for automated security scanning and testing in DevSecOps, 2019, ISBN 1789802024
- Vijay Kumar Velu,Robert Beggs : Mastering Kali Linux for Advanced Penetration Testing: Secure your network with Kali Linux 2019.1 – the ultimate white hat hackers' toolkit, Packt Publishing Ltd, 2019. jan. 30
- Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic,

Ryan Limm, and Stephen Sims: Gray Hat Hacking: The Ethical Hacker's Handbook
- Andrew S. Tanenbaum - David J. Wetherall: Computer networks, ISBN:978-0132126953
- Kevin Mitnick: The Art of Invisibility
- Chris Wysopal: Art of Software Security Testing, The Identifying Software Security Flaws, ISBN 0321304861

Handouts

1. Week 1
2. Week 2
3. Week 3
4. Week 4
5. Week 5
6. Week 6
7. Week 7

Test Questions

1. Define computer security
2. Explain Confidentiality, Integrity and Availability
3. What are the challenges in Computer Security
4. Define attack types
5. Define Threats, Attacks, and Assets
6. Explain Security Requirements
7. Explain Fundamental Security Design Principles
8. Explain Computer Security Strategies
9. Define the basic concepts of cryptographic algorithms: Plaintext, Encryption algorithm, Secret key, Ciphertext, Decryption algorithm
10. Explain Message Authentication and Hash Functions
11. Explain Public-Key Encryption
12. Explain Digital Signatures and Key Management
13. How can public-key encryption be used to distribute a secret key?
14. Explain DES algorithm
15. Explain AES algorithm
16. Explain MD5 algorithm
17. Explain Message Authentication Code
18. What are Malicious software ? What Harm do they cause ? What are the prevention actions you recommend?
19. Explain network penetration testing
20. Define Fundamental Security Design Principles