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

Ütemterv

Week #	Lecture	Labor
Week 1	Alapfogalmak	Labor használati rend, oktatási anyagok
Week 2	Biztonság tervezési alapelvek	Kódolási feladat: funkcionális és nem funkcionális követelmények 1.
Week 3	Támadások kivédése	Kódolási feladat 2.
Week 4	Kali Linux	Alap utasítások
Week 5	Kali linux eszközök	Adat helyreállítási gyakorlat
Week 6	Hálózatbiztonsági ismeretek	Kódolás - biztonságos adattár
Week 8	Bank Holiday	Bank Holiday
Week 9	Malicious code	Virus and malwae checking tools
Week 10	Kriptográfiai algoritmusok 1	Jelszavak tárolása
Week 11	Kriptográfiai algoritmusok 2	Digitális aláírás
Week 12	Kriptográfiai algoritmusok 3	Kódolási gyakorlat
Week 13	Személyes adatok biztonsága	Helyreállítás, törlés
Week 14	Etikus hackelés	Etikus hackelés gyakorlat

Kötelező irodalom

Hornyák Olivér:

Szoftverrendszerek biztonsága

, „FŐNIX ME” – Megújuló Egyetem felsőoktatási intézményi fejlesztések a felsőfokú oktatás minőségének és hozzáférhetőségének együttes javítása érdekében EFOP 3.4.3-16-2016-00015 projekt keretében kidolgozott tananyag

Ajánlott irodalom

- 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
- Muha Lajos; Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése

Oktatási anyagok

1. Week 1
2. Week 2
3. Week 3
4. Week 4
5. Week 5
6. Week 6
7. Week 7
8. Szoftver rendszerek biztonsága

Ellenőrző kérdések

1. Határozza meg a számítógépes biztonság fogalmát
2. Ismertesse a titoktartást, az integritást és a rendelkezésre állást
3. Melyek a számítógépes biztonság kihívásai?
4. Ismertesse meg a számítógépes támadás típusait
5. Fenyegetések, támadások és eszközök meghatározása
6. Magyarázza el a biztonsági követelményeket
7. Ismertesse az alapvető biztonsági tervezési elveket
8. Ismertesse a számítógépes biztonsági stratégiákat
9. Határozza meg a kriptográfiai algoritmusok alapfogalmait: egyszerű szöveg, titkosítási algoritmus, titkos kulcs, titkosított szöveg, visszafejtő algoritmus
10. Magyarázza el az üzenetek hitelesítését és a hash-funkciókat
11. Magyarázza el a nyilvános kulcsú titkosítást
12. Magyarázza el a digitális aláírásokat és a kulcskezelést
13. Hogyan használható a nyilvános kulcsú titkosítás titkos kulcs terjesztésére?
14. Magyarázza el a DES algoritmust

15. Magyarázza el az AES algoritmust
16. Magyarázza el az MD5 algoritmust
17. Magyarázza meg az üzenet hitelesítési kódját
18. Mik azok a rosszindulatú szoftverek? Milyen károkat okoznak? Milyen megelőző intézkedéseket javasol?
19. Magyarázza el a hálózati penetráció tesztelését
20. Az alapvető biztonsági tervezési elvek meghatározása