Tárgyleírás angol nyelvű képzés tárgya esetén

Tárgy neve: Cyber Security Lab II.

Tárgyfelelős neve: Dr. Tihanyi Norbert

Tárgyfelelős tudományos fokozata: PhD

Tárgyfelelős MAB szerinti akkreditációs státusza: AR

Az oktatás célja angolul / Aim of the subject:

The subject covers the fundamentals of Random. Number generators and their related applications . The subject covers the basic principles of penetration testing and malware analysis. Well-known attacks against PKI infrastructures will be demonstrated during the course. . The subject covers the basic principles of modern Kleptography.

Knowledge:

- Students will have comprehensive and up-to-date knowledge and understanding of the general theories and the related concepts of Random Number Generation and analysis.
- Students are familiar with the basic principles of modern malware analysis methods.
- Students will have extensive knowledge on how to analyze source codes to find hidden vulnerabilities
- Students will have extensive knowledge on finding backdoors in PKI infrastructure and certificates.
- vulnerabilities do appropriate penetration testing on complex IT infrastructures

---

Abilities:

- Students are able to apply their mathematical, computer science and informatics skills in order to solve complex cryptographic puzzles and problems.
- They know how to use modern vulnerability assessment tools
- Students will have extensive knowledge on how to identify weaknesses in modern. IT infrastructures

---

Attitude:

- Students are committed to lifelong learning, and are open to acquiring new IT security principles.
- Students follow international standards to solve complex problems related to penetration testing and malware analysis.
- Seeks to collaborate with professionals in other fields.

Autonomy, responsibility:

- Students take responsibility for their professional decisions made in their IT Security related. activities.
- They undertake to meet deadlines and to have deadlines met.
- They bear responsibility for their own work as well as for the work of their colleagues they work together with in a project.
- Regarding mission critical IT systems, they can be entrusted with developing and operational responsibilities that are in accordance with their professional competencies.

Az oktatás tartalma angolul / Major topics:

- PKI systems / RSA / Diffie-Hellman key exchange protocols
- Pollard P-1, Pollard rho factorization methods
- Recovering private keys from public keys using factorization methods (case-studies)
- Hash functions and their applications
- Random Number Generators and their applications (LCG, LSFR, Mersenne Twister)
- NIST Special Publication 800-22

Evaluation:

- The expected knowledge conforms with IREB CPRE and ReBOK.

Irodalom / Literature:

1. Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C
2. Jean-Philippe Aumasson : Serious Cryptography: A Practical Introduction to Modern Encryption
3. Christof Paar and Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners
4. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf
5. David Jonhston: Random Number Generators—Principles and Practices: A Guide for Engineers and Programmers