|  |  |
| --- | --- |
| HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY AND EDUCATION  **Faculty of Information Technology** | **Major : Information Technology**  **Level : Undergraduate**  **Program : High Quality Training** |
|  |  |

**INFORMATION SECURITY   
COURSE SYLLABUS**

1. **Vietnamese name:** An toàn Thông tin
2. **English name:** Information Security **Course number:** INSE340380
3. **Total credits:** 4(3/1/6) (3 Theories + 1 Labs)

Duration: 15 weeks

1. **Instructors:**

* Primary: Nguyễn Đăng Quang,
* Co-lecturers: Huỳnh Nguyên Chính, Nguyễn Thị Thanh Vân

1. **Pre-requisite courses**

Introduction to Programming, Computer network, Database

1. **Course Description**

This course provides students with a consideration of security problems in computing. Topics include:

* Foundations: security mindset, essential concepts (policy, CIA, etc.)
* Software security: vulnerabilities and protections, malware analysis;
* Practical cryptography: encryption, authentication, hashing, symmetric and asymmetric crypto;
* Networks: protocols, attacks and countermeasures;

1. **Course Goals**

|  |  |  |
| --- | --- | --- |
| *Goal* | *Goal description* | *Outcomes* |
| G1 | To provide a comprehensive understanding of Computer Security, Cryptography, Physical Security, Operating System Security, Malware, Network Security, Web security, Security Models and Practice | 1.2, 1.3 |
| G2 | To provide concept-level hand-on experience in specific topic areas. | 2.1, 2.2 |
| G3 | Teamwork, Presentation skill | 3.1, 3.2 |
| G4 | To provide a clear understanding of the security in using computer as well as potential threats to individual privacy that might arise from inappropriate use of computer security technology | 4.3, 4.4 |

1. **Learning outcomes**

|  |  |  |  |
| --- | --- | --- | --- |
| Goals | | Description  *Upon completion of this course, the students should be able to* | Outcomes (CDIO) |
| G1 | G1.1 | To describe the basic concepts of Computer Security, Cryptography | 1.2 |
| G1.2 | To explain Security model practice in Software Security, Network security, Web security. | 1.3 |
| G1.3 | To explain the vulnerability of information system | 1.3 |
| G1.4 | To recognize common attack patterns | 1.4 |
| G2 | G2.1 | To demonstrate understanding about the vulnerability of programs | 2.1 |
| G2.2 | To demonstrate how to detect and reduce threats in Web security | 2.2 |
| G2.3 | To demonstrate the firewall and IDS operation | 2.2 |
| G2.4 | To demonstrate Web application attack and countermeasure | 2.2 |
| G3 | G3.1 | To collaborate and sharing ideas among group members | 3.1 |
| G3.2 | To improve English reading skill | 3.2 |
| G4 | G4.1 | To enhance knowledge on other computing subjects in curriculum | 4.2,4.3 |
| G4.2 | To raise the awareness of students about security issues in learning and working workplaces | 4.4 |

1. **Learning materials:**

* Lecture notes
* Textbooks:

## [1] William Stallings and Lawrie Brown (2014), Computer Security, Principles and Practice, Third Edition

ISBN-10: 0-133-77392-2

[2] Wenliang Du (2017), Computer security a hands-on approach, ISBN-10: 154836794X

* Reference:

[3] Mark Stamp (2011), Information Security, Principle and Practices, 2nd Edition, Wiley Inc. Publication

[4] W. Stallings (2011), Cryptography and Network Security - Principles and Practices. 5th edition, Pearson.

[5] Matt Bishop (2004), Introduction to Computer Security, Prentice Hall,

|  |  |
| --- | --- |
| **ISBN** | : 0-321-24744-2 |

1. **Grading:**

Grading scale: **10**

The following constitutes composition of the final course score:

* Formative assessment: 50%
  + Homework assignments: 30%
  + Group presentation: 20%
* Final Exam: 50%

1. **Plan:**

|  |  |  |
| --- | --- | --- |
| Week No. | Contents | Outcomes |
| 1 | **Chapter 1**: Computer Security Concepts (4/0/8)   1. The Basic Components 2. Computer Security Terminology 3. Security functional requirements 4. Fundamental Security Design Principles 5. Attack Surfaces and attack Trees 6. Computer Security Strategy | G1.2  G1.3  G1.4 |
| **Task for students at home**   * Reading C1 of Textbook [1] * Doing exercises of C1 | G1.3  G3.2  G4.4 |
| 2,3,4 | **Chapter 2: Software & OS Security**  **Software security**   1. Program flaws 2. Vulnerable programs 3. Defensive, Secure programming 4. Buffer overflow   **Practice lab #1**: Experimenting Buffer Overflow Attack with gdb  **OS security**   1. Trusted Computing Base (TCB): Complete mediation, Tamper-proof, Correct 2. Hardware support for memory protection, processor execution modes (system/user modes) 3. OS and Resource Protection:   Authentication, Authorization, Isolation, Separation, OS isolation from application code.   1. Virtualization & Hypervisor Security Issues | G1.2  G1.3 |
| **Task for Student at home**   * Reading C1 of Textbook [2] * Reading C10, C11, C12 of Textbook [1] * Gaining root access via buffer overflow attack & shellcode injection | G1.3  G3.2  G4.3  G4.4 |
| 5,6 | **Chapter 3: Authentication & Access Control**  **Authentication**   1. Authentication Goals 2. Threat modeling of the password 3. Implementing password authentication 4. Hash functions 5. Password Cracking Tools 6. Biometrics   **Access Control**   1. Controlling access to resources 2. Access control policies (DAC, MAC, RBAC) 3. Access Control Matrix 4. Implementing Access Control (ACL, C-List) 5. Unix File Access Control (SetID, SetGID)   **Practice lab #2:** Set-UID Privileged Programs and Attacks (available soon) | G1.2  G1.3  G1.4 |
|  | **Task for Student at home**  **Homework:** Linux/Windows 7 password crack with John the Ripper |  |
| 7 | **Chapter 5: Database Security**   1. Database Threats and the importance of Database Security 2. Database Access Control 3. Attack on Database SQL-Injection 4. SQL Injection Defenses 5. Inference Attacks on Databases 6. Defenses against Inference Attacks on Databases   **Practice lab #3**: SQL Injection | G1.2  G1.3  G1.4 |
|  | **Task at home:**  Implement SQL injection attack |  |
| 8 | **Review & Mid-term Test: Computer Security (C1-C5)** |  |
| 9 | **Chapter 6: Malicious Code**   1. Malware 2. Viruses 3. Worms 4. Modern Malware 5. Botnet & DDoS 6. Botnet Command and Control 7. DNS Based Botnet C&C 8. Advanced Persistent Threat (APT) 9. Malware analysis   **Practice Lab #4:** Practice analyzing malware with sample code from Malware analysis textbook | G1.2  G1.3  G1.4 |
| 10 | **Chapter 7: Firewalls & Intrusion Detection**   1. Defense in Depth 2. Firewalls 3. Firewall Design Goals & Access Policy 4. Packet Filtering firewall 5. Bastion Hosts 6. Personal Firewalls 7. Advanced Firewall Protection 8. Firewall Topologies 9. IDS/IPS   **Practice lab #5:**  Network scan with nmap  Practiceconfiguring packet filtering with IPTables to block/permit specific IP, port, services.. | G1.2  G1.3  G1.4 |
|  | **Task for students at home**  Implement IP Table rules | G1.3  G3.2  G4.2  G4.4 |
| 11 | **Chapter 8: Introduction to Cryptography**   1. Encryption Basics 2. Security Services & Primitive 3. Cryptosystem (Symmetric, Asymmetric) 4. Traditional Ciphers (substitution, transposition) 5. Message integrity & Hash function (MD, SHA) 6. Message Authentication Code (MAC) 7. Digital Signatures & Public key certificate | G1.2  G1.3  G1.4 |
| 12,13 | **Chapter 9: Symmetric Encryption**   1. Block Cipher Scheme 2. Data Encryption Standard 3. Mangler Function 4. S-Box 5. Security of DES 6. Triple DES 7. AES 8. Encrypting a large message (ECB, CBC, CFB, OFB, CTR)   **Practice lab #6**  Secret-key encryption: Encryption with different ciphers & modes | G1.2  G1.3  G1.4 |
| 14 | **Chapter 10: Public Key Encryption**   1. Modular Arithmetic 2. Totienunction 3. Modular Exponentation 4. RSA 5. Diffie and Hellman Key Exchange 6. Key exchange protocol steps   **Practice lab #6**  Public-key encryption: Verify Digital Signature | G1.2  G1.3  G1.4 |
| 15 | **Review Network security & Cryptography** |  |

1. **Ethics:**

Students must demonstrate that they accomplished themselves all exercises and projects. Those students who cheat or commit plagiarism will be imposed punishment such as lower score to zero.

1. **Approval time:**
2. **Approved by:**

|  |  |  |
| --- | --- | --- |
| **Dean of faculty** | **Program Chair** | **Instructor** |

|  |  |  |
| --- | --- | --- |
|  |  |  |