EASTERN MEDITERRANEAN UNIVERSITY
SCHOOL OF COMPUTING AND TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY
COURSE POLICY SHEET

| | | | |
|---|---|---|---|
| **Course Code** | ITEC413 | **Course Title** | Information System Security |
| **Semester** | 2014-2015 Fall | **Language** | English |
| **Category** | AC (Area Core) | **Level** | Forth Year |
| **Workload** | 240 Hours | **Teaching Format** | 3 Hours Lecture, 2 Hours Laboratory |
| **EMU Credit** | (3,0,2) 4 | **ECTS Credit** | 6 |
| **Prerequisite(s)** | | **Course Web** | http://staff.emu.edu.tr/cemyagli/en/teaching/itec413 |

| | | | |
|---|---|---|---|
| **Instructors(s)** | Cem Yağlı | | |
| **e-mail(s)** | Cem.yagli@emu.edu.tr | **Office No:** | CT109 |

## Course Description

This course focuses on basic concepts, principles and practice of Information Systems Security (ISS). It is containing the topics like: Ethics, legality and the need for ISS, overview of networking and operating systems, their vulnerabilities and prevention. Active-passive attacks and their countermeasures. Access, authentication and user privileges. Foot printing. Scanning. Enumerations and system hacking. Trojans and backdoors. Sniffers. Denial of service attacks. Social engineering techniques. Session hijacking. WEB servers and WEB applications, vulnerabilities, attacks and countermeasures. Wireless networks, vulnerabilities, attacks and protection techniques. Malicious programs; viruses, worms, bacteria. Physical security issues. Evading IDS, honey pots and firewalls. Buffer overflow attacks. Cryptography and crypto analysis. Penetration testing methodologies.

## General Learning Outcomes

On successful completion of this course students should be able to:

- Explain the need, carrier opportunities, ethical and legal regularities of studying in ISS.
- Identify the vulnerabilities, the way of exploits, and their countermeasures of the components of Information Systems
- Distinguish the ethical hackers (White hat hackers), grey hat hackers, black hat hackers and identify the legal - illegal activities of hacking.
- Interpret, reproduce and examine ISS policies. Analyse IS vulnerabilities and design-implement-suggest solutions for potential attacks.

## Teaching Methodology / Classroom Procedures

- Each week there are two lecture hours, two lab hours and one tutorial hour.
- During the tutorial sessions, well selected sample problems are solved by the instructor to support the theoretical topics.
- Laboratory sessions are organized in parallel to theoretical study given in classrooms. On the lab sessions, students are solving the coding problems with the supervision of their lab assistant. The lab problems are prepared to support the topics and techniques what students are learning in lecture and tutorial hours. At the end of each lab session, students' works are evaluated and scored by the lab assistant.
- Students are encouraged to use internet to search for various related topics. Lecture notes, Lab descriptions, assignments, and announcements will be posted on the course's web site.

## Course Materials / Main References

***Text Book:***

Rick Lehtinen, G.T. Gangemi Sr., "Computer Security Basics", Second Edition, O'Reilly Media, 2006

***Resource Books:***

1. Kimberly Graves, “CEH Study Guide”, Sybex, 2010
2. Dafydd Stuttard, Marcus Pinto, "The Web Application Hacker’s Handbook", Second Edition, Wiley Publishing Inc., 2011
3. Patrick Engebretson, "The Basics of hacking and penetration testing", Elsevier Inc., 2011
4. Mark Egan,, Tim Mather, "The Executive Guide to Information Security: Threats, Challenges, and Solutions", Addison-Wesley, 2004.
5. Jon Erickson, "Hacking: The Art of Exploitation", 2nd Edition,No Starch Press, 2008.

***Lecture Notes:***

All course materials are also available online in Adobe PDF (Portable Document Format).

| **Weekly Schedule / Summary of Topics** | |
|---|---|
| **1 week** | The ethics, legality and the need of Information Systems (IS) Security.<br>Networking and Operating Systems essentials. Domains in IS. Disaster Recovery Planning. |
| **1 week** | Active-passive attacks and their security countermeasures.<br>Access and authentication. User privileges. Vulnerabilities, type of attacks and countermeasures. |
| **1 week** | Foot printing.<br>Scanning. Ways and tools. |
| **1 week** | Physical security. Security policies, planning, controlling, educating, insuring.<br>Enumerations and System Hacking |
| **1 week** | Trojans, time bombs, and back doors.<br>Malicious programs**:** viruses, worms, bacteria.<br>Sniffers. |
| **1 week** | Denial of Service Attacks (DOS). Distributed DOS Attacks (DDOS).<br>Social Engineering Techniques and countermeasures. |
| **1 weeks** | Session Hijacking techniques and countermeasures.<br>Man in middle attacks. Detection and prevention techniques. |
| **1 weeks** | Hacking WEB Servers.<br>WEB Application vulnerabilities, attacking techniques and countermeasures. |
| **1 week** | WEB based password cracking techniques and tools.<br>Attack to Database Servers. SQL injections attacks and countermeasures. |
| **1 week** | Wireless networks. Vulnerabilities, type of attacks and protection ways. |
| **1 week** | Cryptography and crypto analysis. |
| **1 week** | Evading IDS, honey pots and firewalls.<br>Buffer overflow attacks. |
| **1 week** | Penetration testing methodologies, tools, agreements and legal issues. |

**Requirements**

- Each student can have only one make-up exam. One who misses an exam should provide a medical report or a valid excuse within 3 days after the missed exam. The make-up exam will be done at the end of the term and will cover all the topics. No make-up exam will be given for the quizzes.
- Students who do not pass the course and fail to attend the lectures regularly may be given NG grade.
- You must collect at least 50% of the total Lab-Quiz-Assignments marks in order to pass the course.
- Instructions for the submission of assignments will be posted on the course website. It is each student's responsibility to read and follow the instructions. Failure to follow the submission instructions may result in the

assignment receiving a mark of zero.

- You must have a printed copy of the corresponding “Lab Outline” before coming to the Lab. “Lab Outlines” will be posted on the instructor’s website.

| Method of Assessment | | | | | |
|---|---|---|---|---|---|
| Evaluation and Grading | **Assignments** | **Quizzes** | **Lab** | **Midterm Exams** | **Final Exam** |
| Percentage | 20 % | - | - | 40% | 40 % |