Course Description	
Course Code	YS 428
Course Name	SYSTEM AND NETWORK SECURITY
Prerequisite Courses	
Language of the Course	The English
Course Coordinator	-
Instructor(s)	-
Course Assistants	None
The aim of the course	The aim of this course is to make students proficient in security concepts encountered in computer systems and networks.
Course Content	Security concepts, vulnerabilities, attacks and defense mechanisms in computer systems and networks

Weekly Course Content	
Week 1	Introduction to security concept, review of the application, operating system and network security concepts
Week 2	Errors resulting from misconfiguration of applications, Applications with the right to change the authorization level.
Week 3	"Buffer-overflow" style attacks, detecting buffer overflows, using them in a way that harms security, taking precautions for protection, Basic principles to produce reliable applications and special programming tools that can be used for this purpose
Week 4	Evaluation of “legacy” applications that are poorly written, whose source code cannot be accessed and changed, but which must be used, and “Sandboxing” technique
Week 5	Attacks and protection methods against websites and application programs on these sites
Week 6	Increasing security in applications using cryptography
Week 7	Enhancing security in applications using cryptography (continued)
Week 8	Midterm exam.
Week 9	Ensuring security in remotely accessed file systems (NFS, SMB, SFS), Examination of the methods that can be applied to verify the user identity of the system (simple password protection, Kerberos, LDAP, smartcard, etc.)
Week 10	Detection of entering the system by exploiting a security vulnerability and taking precautions
Week 11	Vulnerabilities in existing network protocols (especially TCP/IP) and necessary measures to close these vulnerabilities
Week 12	Security protocols (IPsec, DNSsec, SBGP, etc.)
Week 13	Security protocols(continued)
Week 14	Special structures (firewall) that restrict the network access right and provide transition protection between the internal and external network
Week 15	Final exam.

Course Learning Outcomes	
1	To learn basic computer and network security concepts and applications.
2	To learn the basic types of threats and attacks on information security.
3	To learn the effects of administrative structures on the implementation of security policies, standards and habits.
4	To learn the basic techniques applied to detect vulnerabilities related to computers and networks.
5	To learn firewall and packet filtering techniques.
6	To learn how to design and implement firewall solutions.
7	To learn the role and importance of cryptography in information security.
8	To learn basic cryptographic algorithms and basic applications of these algorithms.
9	To make a project on computer systems and networking, prepare the relevant presentation document and present it to the class

Contribution of the Course to Program Qualifications		Contribution Level
01	The student will have the ability to apply analytical approach, mathematics and science knowledge in software and engineering issues.	5
02	The student will have the ability to identify, define, formulate and solve a problem in software and computer systems.	5
03	The student will have gains scientific research skills in software and engineering problems, has the ability to design a system, part or process.	5
04	The student will have the ability to use the design capability, techniques and tools required for engineering applications.	5
05	The student will have the ability to design, implement and interpret experimental work and software projects by analyzing the results.	5
06	The student will have the ability to work between disciplines and teamwork.	5
07	The student will have the ability to work in international environments and adapt to different cultures.	1
08	The student will have verbal and written communication skills in Turkish and English.	5
09	The student will have the awareness of the necessity of lifelong learning and the ability to realize it.	1
10	The student will gain knowledge of legal issues with the awareness of professional and ethical responsibility.	5
11	The student will have managerial skills (leadership, organization, time and risk management, quality awareness, efficiency, etc.).	5
12	The student will have the ability to participate in social activities, to acquire regular sports habits and to use time in the best way.	2
13	The student will have the ability to find unusual ways and produce projects.	5
14	The student will have professional self-confidence, being an entrepreneur and taking initiative.	3
15	It is sensitive about the problems of the age and looks after the national interests.	1

ECTS WORKLOAD	Number	Duration (hours)	Number*Duration
Face to face education	14	2	28
Out-of-class study time (pre-study, reinforcement)	0	0	0
Homeworks	1	7	7
Presentation / Seminar preparation	4	1	4
Quizzes	0	0	0
Preparation for midterm exams	1	10	10
midterm exams	1	2	2
Project (Semester assignment)	1	8	8
Lab	0	0	0
field work	0	0	0
Preparation for the final exam	1	15	15
Semester final exam	1	2	2
Research	0	0	0
TOTAL WORKLOAD			**76**
ECTS			3

Evaluation		
SEMESTER EVALUATION	**Number**	**Contribution Percentage**
Midterm	1	20
Quiz	0	0
Homework	1	20

SEMESTER TOTAL		**40**
Contribution rate of mid-term evaluations to success		40
Contribution rate of the final exam to success		60
GRAND TOTAL		**100**

RESOURCES	
Textbook	
Helpful Resources	• Security in Computing, Pfleeger, Charles P., Pearson • Cryptography and Network Security: Principles and Practice, Stallings, William, Prentice-Hall • Operating Systems, Design and Implementation, Tanenbaum, Andrew S., Woodhull, Albert S., Prentice-Hall