General Information:

Name of Course: # ENTERPRISE NETWORK SECURITY

Course Code:	SZE092MN
Semester:	**6**th
Number of Credits:	3
Allotment of Hours per Week:	**2** Lab classes /Week
Evaluation:	Semester grade
Prerequisites:	-

Instructor: **Gábor GYURÁK, assistant lecturer**
Office: H-7624 Pécs, Boszorkány u. 2. Office Nº B-213B
Office hours: www.mik.pte.hu
E-mail: gyurak.gabor@mik.pte.hu

Introduction, General Course Description:

This course describes the architecture, components, operations, and security to scale for large, complex networks, including wide area network (WAN) technologies. The course emphasizes network security concepts and introduces network virtualization and automation.

Learning Objectives:

Students who successfully complete this course will have a comprehensive overview of Enterprise Networking, Security and Autamation.

Students learn how to configure, troubleshoot, and secure enterprise network devices and understand how application programming interfaces (API) and configuration management tools enable network automation.

By the end of this course, students will be able:

- Configure single-area OSPFv2 in both point-to-point and multiaccess networks.
- Explain how to mitigate threats and enhance network security using access control lists and security best practices.
- Implement standard IPv4 ACLs to filter traffic and secure administrative access.
- Configure NAT services on the edge router to provide IPv4 address scalability.
- Explain techniques to provide address scalability and secure remote access for WANs.
- Explain how to optimize, monitor, and troubleshoot scalable network architectures.
- Explain how networking devices implement QoS.
- Implement protocols to manage the network.
- Explain how technologies such as virtualization, software defined networking, and automation affect evolving networks.

Methodology:

- **Practical class**: will give an introduction of planning, building, programming, operating and troubleshooting secure computer networks.

Schedule:

WEEK	TOPIC	Tests
1	Course registration	-
2	Control plane	-
3	OSPF configuration	T1
4	Network Security Concepts	-
5	ACL	T2
6	WAN concepts	-
7	NAT, Firewalls	T3
8	Optimize, Monitor and Troubleshooting	T4
9	Break	-
10	Emerging Network Technologies	T5
11	Practice	-
12	Practice Test	PT
13	Final Exam	FE
14	Retake	RT

Attendance:
Unexcused absences will adversely affect the grade, and in case of absence from more than 30% of the total number of lesson will be grounds for failing the class. To be in class at the beginning time and stay until the scheduled end of the lesson is required, tardiness of more than 20 minutes will be counted as an absence. In the case of an illness or family emergency, the student must notify the lecturer as soon as possible and must present a valid excuse, such as a doctor's note.

Evaluation + Grading:
The course grade is determined as a combination of study-period performance.

Student must complete these parts:
- work with online materials and complete **Group Tests (T1 – T5)**
- pass the **Practice Test (PT)**
- pass the **Final Exam (FE)**

Final grade is calculated:

- T1 4 points (Modules 1-2)
- T2 4 points (Modules 3-5)
- T3 4 points (Modules 6-8)
- T4 4 points (Modules 9-12)
- T5 4 points (Modules 13-14)

  20 points (minimum 5 points)

- PT 40 points
- FE 40 points

  80 points (minimum 40 points)

A total of 100 points can be earned during the semester.

Test scores

Group Test	0-59%	60-69%	70-89%	90-100%
T1	0	1	2	4
T2	0	1	2	4
T3	0	1	2	4
T4	0	1	2	4
T5	0	1	2	4
Group tests total points				**20 points**
Minimum requirement				*5 points*

All exams and tests are closed-book and closed-notes. Any students who do not take the examination at the scheduled time will receive a zero score.

Retake Test (RT) of the Final Exam (FE) and Practice Test (PT) is possible at the 15th week. There is no possibility to retake the Group Tests (T1-T5).

Grade:	5	4	3	2	1
Evaluation in percent:	85%-100%	75%-84%	65%-74%	41%-64%	0-40%

PTE Grading Policy:
Information on PTE's grading policy can be found at the following location:
www.pte.hu

Students with Special Needs:

Students with a disability and needs to request special accommodations, please, notify the Deans Office. Proper documentation of disability will be required. All attempts to provide an equal learning environment for all will be made.

Readings and Reference Materials:

1. William Stallings, Lawrie Brown - Computer Security Principles And Practices (2nd edition), Pearson, 2011.

2. Randy Weaver - Guide to Tactical Perimeter Defense: Becoming a Security Network Specialist, Cengage Learning, 2007.