COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security of LAN and WAN Networks [S1Cybez1>BSLiW]

Course

Field of study
Cybersecurity

Year/Semester
3/5

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
24

Laboratory classes
16

Other
0

Tutorials
0

Projects/seminars
16

Number of credit points

4,00

Coordinators

dr hab. inż. Maciej Sobieraj
maciej.sobieraj@put.poznan.pl

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

Lecturers

Prerequisites

Knowledge of the functioning of local and wide-area packet networks; ability to configure network devices.

Course objective

• Acquire advanced knowledge of modern threats and techniques for securing LAN and WAN networks. • Develop practical skills in configuring and managing dedicated security systems from various vendors. • Prepare for designing and implementing comprehensive security solutions in network environments. • Learn about modern technologies and tools dedicated to protecting network infrastructure.

Course-related learning outcomes

Knowledge:
• Understands advanced network threats and attacks, as well as methods to counteract them. [K1_W10]
• Has knowledge of the operation and configuration of modern security systems (NGFW, IPS, ATP).

[K1_W07]
• Is familiar with security solutions provided by Cisco, Palo Alto Networks, Check Point, and Juniper. [K1_W20]

Skills:
• Can configure and manage advanced network security devices. [K1_U02]
• Is able to design comprehensive security systems for LAN and WAN networks. [K1_U11]
• Can integrate various security technologies and systems into a cohesive solution. [K1_U11]

Social competences:
• Understands the need for continuous learning in the rapidly evolving field of network security. [K1_K01]
• Can work effectively in a team on advanced security projects. [K1_K05]
• Is aware of the responsibility for information and infrastructure security within an organization. [K1_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

1. Knowledge: A written exam including open-ended and multiple-choice questions on advanced security technologies.
2. Skills: Evaluation of laboratory tasks and group projects based on accuracy, efficiency, and innovation of applied solutions.
In each form of the course assessment, the grade depends on the number of points the student earns relative to the maximum number of required points. Earning at least 50% of the possible points is a prerequisite for passing. The relationship between the grade and the number of points is defined by the Study Regulations. Additionally, the course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university's electronic systems and during the first class meeting (in each form of classes).

Programme content

The course "Security of LAN and WAN Networks" provides students with advanced knowledge and practical skills in securing local (LAN) and wide area (WAN) networks. The course focuses on identifying advanced threats, implementing modern security technologies, and configuring dedicated systems offered by leading vendors such as Cisco, Palo Alto Networks, Check Point, and Juniper Networks. Students will learn advanced network protection techniques, including Next-Generation Firewalls (NGFW), Intrusion Prevention Systems (IPS), Advanced Threat Protection (ATP), and Identity and Access Management (IAM) solutions.

Course topics

I. Advanced Network Threats and Attacks (4x45 minutes)
1. Modern Network Threats
• Advanced Persistent Threats (APT) attacks.
• Ransomware, botnets, and multi-vector malware.
• Attacks on network infrastructure: BGP hijacking, DNS spoofing.
2. Current Security Solutions
• Overview of security technologies from Cisco, Palo Alto Networks, Check Point, Juniper.
• Introduction to security standards (ISO/IEC 27001, NIST).
II. Advanced Techniques for Securing LAN Networks (6x45 minutes)
1. Layer 2 Security
• Protection against ARP spoofing and MAC flooding attacks.
• Port Security techniques in Cisco and Juniper devices.
• Implementation of DHCP Snooping and Dynamic ARP Inspection.
2. Authentication and Access Control
• Deployment of 802.1X using Cisco Identity Services Engine (ISE).
• Network Access Control (NAC) solutions from Juniper (Juniper Unified Access Control).
• Identity management using Active Directory and LDAP.
3. Network Segmentation

• Microsegmentation using VLAN and Private VLAN technologies.
• Implementation of Virtual Routing and Forwarding (VRF) in Cisco devices.
III. Advanced Techniques for Securing WAN Networks (6x45 minutes)
1. Next-Generation Firewalls (NGFW)
• Concept of NGFW and their role in network security.
• Configuration and management of Cisco Firepower, Palo Alto Networks NGFW, and Check Point Quantum Security Gateways.
2. Intrusion Detection and Prevention Systems (IPS)
• Implementation of IPS in Cisco (Firepower), Palo Alto Networks (Threat Prevention), and Juniper (Junos IPS) devices.
• Analysis of network anomalies and signature-based threat detection.
3. Advanced Virtual Private Networks (VPN)
• VPN technologies: IPSec, SSL/TLS, FlexVPN.
• Implementation of site-to-site and remote access VPNs using Cisco AnyConnect and Palo Alto GlobalProtect.
• Application of GETVPN in corporate environments.
IV. Modern Security Systems and Technologies (8x45 minutes)
1. Advanced Threat Protection (ATP)
• Use of Cisco Advanced Malware Protection (AMP).
• Palo Alto Networks WildFire and Check Point SandBlast.
• File analysis and sandboxing to detect advanced threats.
2. Security Management and Event Analysis
• SIEM systems: Splunk, IBM QRadar.
• Integration of security devices with SIEM.
• Log analysis and event correlation.
3. Application Control and Content Filtering
• Implementation of Application Control in NGFW.
• URL filtering and network-level antivirus solutions.
• Protection against web threats using Secure Web Gateway (SWG).

Teaching methods

• Lectures: Multimedia presentations with practical examples and case studies, online.
• Laboratories: Hands-on exercises using devices and software from various vendors.
• Project: Teamwork on a comprehensive network security solution.

Bibliography

Basic:
1. Santos, O., Kampanakis, P., & Woland, A. (2016). Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. Cisco Press. ISBN: 9781587144462.
2. Official Cisco documentation for ASA, Firepower, and ISE available at:
o Cisco ASA
o Cisco Firepower
o Cisco ISE
3. Piens, T. (2022). Mastering Palo Alto Networks: Build, configure, and deploy network solutions for your infrastructure using features of PAN-OS (2nd ed.). Packt Publishing. ISBN: 9781803241418.
4. Palo Alto Networks training materials available at: Palo Alto Networks Education.
5. Check Point Firewall Administration R80.10 - Guide available at: Check Point R80.10 Administration Guide.
6. Check Point Infinity documentation available at: Check Point Infinity Documentation.
7. Woodberg, B., & Cameron, R. (2013). Juniper SRX Series: A Comprehensive Guide to Security Services on the SRX Series. O'Reilly Media. ISBN: 9781449339029.
8. Juniper Networks technical documentation available at: Juniper Networks Technical Documentation.

Additional:
1. Documentation and whitepapers from network device and solution manufacturers.
2. Educational materials prepared by the instructors.

Breakdown of average student's workload

	Hours	ECTS
Total workload	116	4,00
Classes requiring direct contact with the teacher	56	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	60	2,00