

Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT
Department: INFORMATION TECHNOLOGIES
Professional Field: 5.3 COMMUNICATION AND COMPUTER TECHNOLOGY
Specialty: CYBER SECURITY OF COMMUNICATION TECHNOLOGIES
Educational-qualification degree: BACHELOR

LEARNING COURSE DESCRIPTION

1.Course title: Workshop on server security

2.Course code: B.43.060.1

3.Type of the course: compulsory

4.Level: Bachelor

5.Year of study: 4

6.Semester: 8

7.Number of credits: 3

8.Name of the lecturer: Assist. Prof. Strahil Sokolov, Eng. PhD

9.Course learning outcomes:

The aim of the course is to provide the students of the special CCT of VUTP with practical skills for the protection of server OS and web servers.

Students who have completed their studies in the discipline must acquire:

Basic knowledge of how to protect servers from various types of attacks.

Practical skills to configure and prevent heterogeneous attacks.

Competencies:

- configuring server and components for compliance with security policies;
- creation of protection policies;
- organizing server security management activities.

10.Teaching methods:

The training in the discipline "Server Protection Practicum" is carried out in the sixth semester according to the effective curriculum of the CSVT specialty through practical exercises grouped in a block of 3 hours during the semester.

Practical exercises are conducted in the classic way, with the students becoming familiar with the intended material in sequence. The statements are illustrated with examples that make the students' work in the exercises as easy as possible. Practical exercises are conducted in a laboratory or on the student's own computer, equipped with the necessary equipment - hardware and server operating system. Before each practical lesson, students are informed about the need for preliminary preparation on the relevant topic.

11. Prerequisites:

Students should have in-depth knowledge of Linux OS, Windows Basics, Web Servers, Network Load Balancing.

12. Course contents:

Introduction to the course is studied in the course. Basics of cloud computing and architectural The course "Practicum on server protection" for special CSVT of VUTP contains three sections. Securing Linux Servers is presented in Section 1. The following modules are part of the intended practical training: User and Network Management. Protection of confidential user data. Management and protection of a data storage system. Cloud technologies and configuring firewalls. Management and security of hypervisor and applications in containers. Management security of tools for transfers, sharing of confidential data. DNSSEC and protected from DDoS attacks. Built in surveillance system. Management and protection of centralized authentication services through auto-identification and authorization. Management of VPN, SSH and TOR services. Section 2 presents Securing Windows Servers: Installation and User Management. Disk space management and encryption. Manage server roles. Windows hypervisor and container management and security. Building a monitoring system. Section 3 presents Securing WEB Servers with the following subtopics: Managing Apache httpd. Manage nginx. Installation and configuration of modules. Management of IIS7.0 IIS7.5. Installation.

Role management. Installing modules. SSL/TLS termination. Building a monitoring system, building security policies and security testing tools.

13. Bibliography

Basic literature:

1. Chris Binnie, "Linux Server Security: Hack and Defend", ISBN 1119277655, 9781119277651, ISBN 1119277655, 9781119277651
2. Jordan Krause, "Windows Server 2016 Security, Certificates, and Remote Access Cookbook: Recipe-based guide for security, networking and PKI in Windows Server 2016", ISBN 1789135222, 9781789135220, Packt Publishing Ltd, 2018
3. Gerardus Blokdyk, "Server Security a Complete Guide - 2020 Edition", ISBN 1867344688, 9781867344681, Emereo Pty Limited, 2020

Additional literature:

1. Axel Buecker, Kent Browne, Louis Foss, Jaco Jacobs, Vladimir Jeremic, Carsten Lorenz, Craig Stabler, Joris Van Herzele, IBM Redbooks, "IBM Security Solutions Architecture for Network, Server and Endpoint", ISBN 0738435430, 9780738435435, IBM Redbooks, 2011
2. Gerardus Blokdyk, "Server Security Complete Self-Assessment Guide", ISBN 0655521291, 9780655521297, Emereo Pty Limited, 2019
3. John R. Vacca, "Cyber Security and IT Infrastructure Protection", ISBN 0124200478, 9780124200470, Syngress, 2013

14. Assessment methods and criteria:

The final grade in the discipline is formed through a final test. The written test covers open and closed questions on the material specified in the synopsis and presented in the lectures on the subject.

The criteria are: comprehensiveness, accuracy and thoroughness in answering the questions asked in the test.

The subject test consists of up to 60 questions. The answer to each question in the test is evaluated. Comprehensive, accurate and thorough development of a test question is assessed with 10 points. Maximum number of points – 100.

The obtained assessment from the current control (formed by the points from the practical exercises and the conducted control works to check the theoretical and practical assimilation) and the assessment from the written exam are transformed into a final assessment according to the six-point system.

Forming the final grade

The formation of the final grade is formed by an assessment from the written test and an assessment from the current control (points from the laboratory exercises and the conducted control works to check the theoretical and practical assimilation).

The formation of an assessment in the training course at each of the specified stages, according to the obtained points and their arrangement according to the six-point system, is given in Table 1.

Table 1.

Number of points	Assessment According to the 6-point Scale System
0 – 20	Fail 2 (F)
20 – 39	Fail 2 (FX)
40 – 49	Satisfactory 3.00 (E)
50 – 59	Satisfactory 3.00 (D)
60 – 69	Good 4.00 (C)
70 – 84	Very good 5.00 (B)
85 – 100	Excellent 6.00 (A)

15. Language of instruction: Bulgarian/English