

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

LEARNING COURSE DESCRIPTION

1. Course title: HACKING ATTACKS AND TOOLS

2. Course code: P.18.036.1

3. Type of the course: *compulsory*

4. Level: professional bachelor

5. Year of study: 3

6. Semester: 5

7. Number of credits: 6

8. Name of the lecturer: Assoc. Prof. Dr. Eng. Ivan Ivanov

9. Course learning outcomes:

The aim of the course is to give the students in a systematized form basic knowledge in the field of hacker attacks and tools.

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

Basic knowledge of types of penetration testing, their classification and methodology for testing vulnerabilities in web applications, databases, mobile applications, wireless networks, VLANs and VPNs.

Practical skills for the Kali Linux tools for vulnerability testing as well as testing with free penetration tools.

Competencies: Upon completion of the course, students should have mastered the mechanisms and tools of vulnerability testing.

10. Teaching methods:

The teaching method is a discussion form, according to the specifics of the matter under consideration. Emphasis is placed on key issues related to hacking attacks and tools, and multimedia is used.

11. Prerequisites:

Students should have in-depth knowledge of Security Fundamentals and Information Security Standards, Cyber Threats and Cyber Crises and Cyber Security Policies.

Courses using the discipline are: Information Security Management, Secure Network Design and Server Protection

12. Course contents:

Current topics related to the history, development and methodology of testing are considered in the course. Types of penetration tests, penetration tools and their classification. . Students analyze wireless network penetration tests, analyze VLAN penetration tests, as well as VPN penetration tests. It examines methodology and classification for testing vulnerabilities in web applications, databases, mobile applications, wireless networks, and VPNs. During the training, skills are acquired in using the tools in Kali Linux for testing for vulnerabilities, as well as testing with free penetration tools.

13. Bibliography

Basic literature:

1. Georgia Weidman, Penetration Testing: A Hands-On Introduction to Hacking, No Starch Press; 1st edition (June 14, 2016).
2. Gus Khawaja, Kali Linux Penetration Testing Bible, Wiley; 1st edition (May 14, 2021).
3. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Wiley; 2nd edition (September 27, 2017).
4. Andress J. The Basics of Information Security, Second Edition: Understanding the Fundamentals of InfoSec in Theory and Practice 2nd Edition, Syngress, 2014.

5. Conklin W. A, White G, Cothren C, Davis R, Williams D, Principles of Computer Security, Fourth Edition (Official Comptia Guide) 4th Edition, McGraw-Hill Education, 2015.

Additional literature:

1. Ivanov I. Manual for laboratory exercises on information security and protection and administration and protection of communication and computer networks, ed. center-VU KTP, Sofia, 2013, ISBN: 978-954-9332-88-9.
2. Partyka T. JI, Popov I. I. Information security: textbook / T. JI. Partyka, I. I. Popov. — 3rd ed., revised. and add. — M.: FORUM, 2010.
3. Gribunin V, G, Chudovsky V. V, Kompleksnaya sistema zashtiya information na przes, Publishing center "Academy", 2009.
4. Meeuwisse R, Cybersecurity for Beginners, Cyber Simplicity Ltd, 2017.
5. Kim D, Solomon M, Fundamentals of Information Systems Security 3rd Edition, Jones & Bartlett Learning, 2016.

14. Assessment methods and criteria:

The evaluation of the discipline is formed through a point system, the maximum number of points that students can receive is 100 (see table 1). Knowledge, skills and competence are evaluated by conducting written control works to check the theoretical and practical assimilation of the learning material, the performance of the students during the practical exercises, as well as their ability to independently solve the tasks set in the practical exercises. The discipline ends with a written exam.

Table 1.

Number of points	Assessment According to the 6-pointScale 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*