|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Студијски програм: ОАС ИТ** | | | | |
| **Назив предмета: БЕЗБЕДНОСТ И ЗАШТИТА РАЧУНАРСКИХ МРЕЖА** | | | | |
| **Наставник: Марјан Д. Милошевић** | | | | |
| **Статус предмета: И** | | | | |
| **Број ЕСПБ: 6** | | | | |
| **Услов: Рачунарске мреже и комуникације, Заштита података** | | | | |
| **Циљ предмета**  Упознавање са фундаментима безбедности рачунарских мрежа, облицима претњи и напада, безбедносним  протоколима, методама заштите мрежне инфраструктуре и интернет сервиса, имплементацијом софтвера за  заштиту и применом различитих алата за тестирање безбедности рачунарске мреже, пројектовањем безбедносних решења, регулативама, стандардима, као и етичким аспектима злоупотребе рачунарских ресурса. | | | | |
| **Исход предмета**  Очекује се да студент:  - самостално врши анализу ризика у умреженим рачунарским системима  - користи криптографске, организационе и друге облике заштите рачунарских ресурса  - тестира безбедност мрежних сервиса  - инсталира и конфигурише софтвере за заштиту рачунарске мреже и мрежних сервиса | | | | |
| **Садржај предмета**  *Теоријска настава*  Облици напада на мрежи. Безбедносна политика и механизми заштите. Анализа ризика. Криптографске  методе заштите. Симетрично и асиметрично шифровање. Дигитални потпис и дигитални сертификат.  Аутентификација порука. Виртуелне приватне мреже и IPSec. Мрежне баријере и системи за детекцију  упада. Безбедност Web-a. Безбедност бежичних мрежа. Организационе мере заштите. Етички хакинг.  Безбедност и рачунарство у облаку. Безбедност и интернет интелигентних уређаја  *Практична настава*  Безбедносно тестирање мреже и сервера и извођење напада у контролисаном, лабораторијском окружењу.  Примена мера заштите на различитим слојевима TCP/IP. Имплементација криптографских протокола (TLS,  SSH). Инсталација и конфигурисање софтвера за заштиту. Конфигурација мрежне баријере под оперативним  системом Linux. Конфигурација система за детекцију упада. Студије случајева напада и заштите. | | | | |
| **Литература**  [1] Stallings W., Osnove bezbednosti mreža: aplikacije i standardi, CET, Beograd, 2014, ISBN 978-86-7991-376-0.  [2] Stallings W., Cryptography and Network Security: Principles and Practice, Pearson, 2023, ISBN: 1-292-43748-0  [3] Wenliang Du: Computer & Internet Security: A Hands-on Approach, Third Edition, 2022, ISBN: 978-1733003940  [4] Плескоњић Д., Ђорђевић Б., Мачек Н., Царић М., Сигурност рачунарских система и мрежа,  Микрокњига, Београд, 2007, ISBN 978-86-7555-305-2  [5] Јевремовић A., Веиновић М., Шарац М, Шимић Г., Заштита у рачунарским мрежама, Универзитет Сингидунум, Београд, 2018, ISBN 978-86-7912-565-1  [6] Forshaw J, Napadi na mrežne protokole: Hakerski vodič za hvatanje mrežnog saobraćaja, analizu i  iskorišćavanje ranjivosti mreže, Mikroknjiga, 2018, ISBN 978-86-7555-429-5  [7] J.F.Kurose, K.W.Ross, Computer Networking: A Top-Down Approach, Eight Edition, Pearson, 2020, ISBN: 9780135928615 | | | | |
| **Број часова активне наставе** | **Теоријска настава: 2** | | **Практична настава: 2** | |
| **Методе извођења наставе**  Реализација предавања по моделу интерактивне наставе уз коришћење метода практичног рада. Пројектна метода. Метода демонстрације и студије случаја. | | | | |
| **Оцена знања (максимални број поена 100)** | | | | |
| **Предиспитне обавезе** | поена | **Завршни испит** | | поена |
| активност у току предавања | / | писмени испит | | 30 |
| практична настава | / | усмени испит | | 20 |
| колоквијум-и | 30 |  | |  |
| семинар-и | 20 |  | |  |