Студијски програм : МАС ИТ

Назив предмета: ЗАШТИТА РАЧУНАРСКИХ СИСТЕМА

Наставник/наставници: Марјан Д. Милошевић

Предавач из привреде: Срђан Атанасијевић

Статус предмета: Изборни

Број ЕСПБ: 6

Услов: Уписан одговарајући семестар

Циљ предмета

Рад са основним концептима заштите рачунарских система. Упознавање студената са новим безбедносним претњама и ризицима, као и са техникама заштите рачунарских система на конкретним примерима. Повећање нивоа свести о могућим претњама и нападима пре свега у Интернет окружењу, као и проширивање сазнања о новим алатима за детектовање рањивости постојећих система, моделовање претњи и примену превентивне заштите. Упознавање са актуелним европским стандардима о приватности података.

Исход предмета

Студенти ће умети да изврше моделовање претњи у модерним информационо-комуникационим системима, да примене специјализоване софтвере за детекцију и елиминисање напада, да самостално дефинишу периметарске методе заштите, врше анализу злонамерних софтвера и имплементирају мере заштите у различитим фазама развоја софтвера.

Садржај предмета

Теоријска настава

Увод у заштиту рачунарских система. Безбедносне претње и ризици. Анализа методологије нападача. Механизми контроле приступа. Методологије моделовања претњи. Модели заштите. Физичка заштита. Хардверска заштита. Криптографске методе заштите. Дигитални потпис и дигитални сертификати. Заштита рачунарских мрежа. Заштита апликација. Безбедност Интернета-ствари. Анализа злонамерног софтвера.

Практична настава

Примена метода друштвеног инжењеринга. Методе управљања ризиком. Методе phishing-а. Примери вируса и антивирусног софтвера и софтвера за анализу злонамерних програма. Примери примене криптографије. Примери примене дигиталног потписа и стеганографија. Методе аутентификације Примена ПКИ. Примена firewall-ова, Пентестинг.

Литература

1. Д. Плескоњић, Н. Мачек, Б.Ђорђевоћ, М.Царић, Сигурност рачунарских система и мрежа, Микро књига. Београд, 2007.
2. J.Farshaw, Напади на мрежне протоколе, хакерски водич за хватање мрежног саобраћаја, анализу и искоришћавање рањивости мреже, Микрокњига, Београд, 2018
3. G. Najera-Gutierrez, J.A. Ansari, Kali Linux тестирање непробојности веба, треће издање, Компјутер библиотека, Чачак, 2018.
4. Ауторизована предавања доступна на сајту за е-учење (http://eucenje.ftn.kg.ac.rs)

Број часова активне наставе	**Теоријска настава:** 30	**Практична настава:** 30

Методе извођења наставе

Методе популарног предавања, студија случаја, дискусија, практичан рад, индивидуални рад на рачунару, пројектни рад.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	поена	**Завршни испит**	поена
активност у току предавања	5	писмени испит	30
практична настава	5	усмени испт	20
колоквијум-и		.....	
семинар-и	40		

Начин провере знања могу бити различити наведено у табели су само неке опције: (писмени испити, усмени испт, презентација пројекта, семинари итд.....

*максимална дужна 2 странице А4 формата