Студијски програм: Основне академске студије информатике

Назив предмета: ИНФОРМАЦИОНА БЕЗБЕДНОСТ

Статус предмета: Обавезан на свим модулима Основних академских студија информатике

Број ЕСПБ: 5

Услов: Уписан одговарајући семестар

Циљ предмета

Циљ предмета је да студентима обезбеди свеобухватно разумевање информационе безбедности – од основних принципа и организационих политика до практичне примене одбрамбених и офанзивних техника у сајбер окружењу. Студенти се оспособљавају за идентификацију, процену и ублажавање ризика, као и за пројектовање, имплементацију и тестирање безбедносних механизама у складу са важећим стандардима и регулативама.

Исход предмета

Студент је способан да идентификује и процени безбедносне ризике и рањивости у ИКТ системима, примени мере заштите, политике и контролне оквире, спроведе активности реаговања на инциденте у SOC окружењу, изврши пенетрационо тестирање и анализу безбедности апликација, разуме правни, регулаторни и етички контекст информационе безбедности и учествује у развоју и имплементацији безбедносних стратегија.

Садржај предмета

Теоријска настава

Принципи информационе и сајбер безбедности (поверљивост, интегритет и доступност). Управљање ризицима и политикама безбедности. Контролни оквири и стандардизација (NIST CSF, COBIT, CIS Controls, ISO/IEC 27001, MITRE ATT&CK). Правни и регулаторни оквир (GDPR, NIS2, CyberSecurity Act, DORA, SOC Reports). Управљање логовима, мониторинг догађаја и улога SOC-а. Реаговање на инциденте и опоравак од катастрофа. Основе офанзивне безбедности: откривање рањивости, пенетрационо тестирање и технике напада. OWASP Top 10 и врсте рањивости у веб апликацијама. Безбедносна култура, етика и питања људских ресурса у безбедности.

Практична настава:Вежбе

Анализа логова и мрежног саобраћаја. Употреба алата SOC-а: SIEM, SOAR, EDR, XDR. Пенетрационо тестирање веб апликација и API-ја. Ревизија и процена усклађености безбедносних политика. Примена аутентификационих механизама (MFA, SSO, PAM). Симулирање активности црвеног и плавог тима. Дизајн безбедносног оквира за модел организације.

Литература

1. Security Engineering: A Guide to Building Dependable Distributed Systems, Ross J. Anderson, Wiley (2020)
2. Security Operations Center – Building, Operating, and Maintaining your SOC, Joseph Muniz et al., Cisco Press (2015)
3. The Web Application Hacker’s Handbook, Dafydd Stuttard, Marcus Pinto, Wiley (2020)
4. Red Team Field Manual, Ben Clark, Createspace (2014)
5. CISM All-in-One Guide, Peter H. Gregory, McGraw-Hill (2018)

Број часова активне наставе	**Теоријска настава:** **3**	**Практична настава:** **2**

Методе извођења наставе

Проблемски-оријентисана настава, практична настава, самостални рад студената, консултације. Практичан рад на симулаторима различитих напада на виртуелном окружењу.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	**70** поена	**Завршни испит**	**30** поена
Практична настава	5	усмени испит	30
Колоквијум-и	25+25		
Домаћи задаци	15		

Напомена:

Како је наведено у Табели 10.2, за извођење наставе на овом предмету доступан је сервер.Карактеристике сервера су следеће: HP ProLiant DL360 Gen9, 2 x Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz, 64 GB, 2TB.