



Студијски програм: КП Сајбер безбедност			
Назив предмета: ОСНОВЕ БЕЗБЕДНОСТИ ОПЕРАТИВНИХ СИСТЕМА И МРЕЖА			
Наставник/наставници: Милош Р. Ивановић, Богдан Ж. Милићевић			
Статус предмета: Обавезни			
Број ЕСПБ: 5			
Услов: Нема формалног услова			
Циљ предмета Обезбедити стицање практичних вештина, уз неопходно теоријско знање из области оперативних система и уграђених безбедносних механизма, као и умрежавања, као основу за специјализоване курсеве који следе.			
Исход предмета Студенти разумеју основну улогу ОС-а и концепте безбедности програма и података. Оспособљени су да оперишу командном линијом и скриптама. Поседују практичне вештине за рад на симулатору и примену основних безбедносних принципа на Layer 2 и Layer 3 мрежним уређајима. Способни су да препознају, а и решавају неке проблеме који се односе на безбедност ОС-а и локалне мреже.			
Садржај предмета Теоријска настава Основе оперативних система. Увод у оперативне системе. Упознавање са основним концептима и функционисањем. Корисничке и администраторске одговорности. Процеси, нити, асинхроно извршење. Виртуелна меморија, механизми заштите. Фајл системи, дозволе. Системски сервиси, зависности између системских сервиса, инит процес. Основни појмови виртуелизације и контејнеризације. Основе безбедности оперативних система. Увод у безбедност података (Data Security). Аутентификација на савременим UNIX системима, ауторизација, PAM модули, Mandatory Access Control, Discretionary Access Control, ескалација привилегија, ACL листе, ROC, ASLR механизми. Security Arhitecture и модели безбедности (Bell-LaPadula, Biba, Zero Trust, NIST framework, итд.) Основе рачунарских мрежа. Локалне и регионалне мреже. Комуникације и умрежавање: мрежни стандарди и организације за стандардизацију. ISO референтни модел са 7 слојева. TCP/IP референтни модел са 5 слојева. Физички слој Слој везе података, MAC подслој, VLAN, бежичне технологије. Мрежни слој, IP, IPv6, ICMP, NAT, ARP, DHCP протоколи. Транспортни слој, TCP, UDP протоколи, сокет програмирање. Апликативни слој, HTTP, SMTP, POP3, IMAP, SSH протоколи. Апликације у клијент/сервер окружењу. Основе безбедности рачунарских мрежа. Преглед метода идентификације, блокирања и превенције малициозног мрежног саобраћаја. Безбедност мрежних уређаја (свич, рутер, firewall). WEP/WPA, ARP spoofing, MAC spoofing. Основна подешавања Linux firewall-a iptables. Рањивости протокола за динамичко рутирање. DNS сервис и његове рањивости. Trasport Layer Security. Практична настава Увод у Shell команде и скрипте. Системски сервиси, зависности између системских сервиса. Асинхроно извршење. UNIX иницијализациона секвенца. Практично извођење buffer overflow, ескалације привилегија, ROC. Практични рад на симулаторима GNS3 и Cisco Packet Tracer. Безбедност мрежних уређаја Switch, VLAN, разни сервиси и сервери (NAT, ICMP, DNS, DHCP, FTP, HTTP, SMTP, IMAP), софтвер за мониторинг и администрацију мрежа. Практично извођење базичних мрежних напада.			
Литература 1. W. Stallings, Operating Systems: Internals and Design Principles, Fifth Edition, Pearson Education Inc, 2005. 2. A.S. Tanenbaum, Računarske mreže, Mikro knjiga, Beograd, 2005. 3. Stallings W., Brown L.: Computer security: principles and practice, Prentice Hall, 2007, ISBN 9780136004240 4. Stallings W.: Cryptography and Network Security. Principles and Practice, fifth edition, Prentice Hall, 2011, ISBN 978-0136097044			
Број часова активне наставе		Теоријска настава: 20	Практична настава: 20
Методе извођења наставе Настава се изводи on-line коришћењем ZOOM или Microsoft Teams платформе.			
Оцена знања (максимални број поена 100)			
Предиспитне обавезе		поена	Завршни испит
Кратки тестови		10 (10 x 1 поен)	поена
Практични задаци		60 (5 x 12 поена)	усмени испит
			30





Студијски програм: КП Сајбер безбедност			
Назив предмета: УВОД У РАЗВОЈ И БЕЗБЕДНОСТ ВЕБ АПЛИКАЦИЈА			
Наставник/наставници: Владимир М. Цвјетковић , Андреја И. Живић , Ненад Р. Андрејевић			
Статус предмета: Обавезни			
Број ЕСПБ: 5			
Услов: Нема формалног услова			
Циљ предмета Циљ предмета је обезбедити студентима разумевање принципа и технологија у развоју безбедних веб апликација. Студенти ће стећи знања о веб протоколима, програмирању у JavaScript-у, основама backend-а, и примени сигурних техника кодирања и управљања идентитетом. Циљ је развити способности за развој безбедних веб апликација које испуњавају савремене стандарде безбедности.			
Исход предмета Студент разуме и уме да примени основне принципе и технологије у развоју безбедних веб апликација. Разуме и уме да примени технике безбедног развоја софтвера. Разуме принципе аутентификације и ауторизације, сигурности база података и примењује их у развоју безбедних веб апликација.			
Садржај предмета <i>Теоријска настава</i> Протоколи, технике комуникације. HTTP, HTTP/2, HTTPS протокол. Праћење сесије у HTTP протоколу. Појам колачића (cookie). Слање параметара и слање датотека. Основни концепти програмирања у JavaScript-у. DOM стабло, преглед и модификација из JavaScript-а. Концепт REST-а. Размена података употребом JSON формата. AJAX позиви. Основна окружења за backend програмирање. Рањивост софтвера – дефиниција и уобичајене врсте рањивости (Injection Flaws, Information Leakage and Improper Error Handling, Cross-Site Scripting, Nontechnical Vulnerabilities). Преглед метода за откривање рањивости током развоја софтвера. Сигурне технике кодирања (Validate Input, Validate Output to Be Displayed on Browsers, Keep It Simple, Follow the Principle of Least Privilege, Defense in Depth, Quality Assurance, Coding Standards, Security Requirements, Threat Modeling). Увод у управљање идентитетима и приступима (принципи аутентификације и ауторизације). Принципи сигурности база података (SQL injection, дозволе, сигурност сторних процедура). <i>Практична настава</i> Развој једноставне клијент-сервер апликације по задатом и слободном протоколу. Праћење корисника. Креирање једноставних веб сервера. Основне поставке серверског дела веб апликације (backend). Улога SQL i NoSQL база података у веб апликацији. Праћење сесије, регистрација и пријава на сајт. Слање фајлова на сервер. Употреба REST-а у комуникацији између клијентског и серверског дела кроз AJAX позиве. Демонстрација сигурних техника кодирања. Израда пројектног задатка који укључује израду једноставне веб апликације на коју су примењене сигурне технике кодирања.			
Литература 1. Sullivan B. Liu V. & Howard M. (2012). Web application security : a beginner's guide. McGraw-Hill. 2. Stuttard D. & Pinto M. (2011). The web application hacker's handbook : finding and exploiting security flaws (2nd ed.). Wiley			
Број часова активне наставе		Теоријска настава: 20	Практична настава: 20
Методе извођења наставе Настава се изводи on-line коришћењем ZOOM или Microsoft Teams платформе.			
Оцена знања (максимални број поена 100)			
Предиспитне обавезе	поена	Завршни испит	поена
Кратки тестови	10 (10 x 1 поен)	усмени испит	30
Пројектни задатак	60 (5 x 12 поена)		



Студијски програм: КП Сајбер безбедност			
Назив предмета: ПРИНЦИПИ САЈБЕР БЕЗБЕДНОСТИ			
Наставник/наставници: Ненад Д. Филиповић , Ана М. Капларевић-Малишић , Данило Б. Савић , Јован Р. Богићевић , Бранко С. Суботић			
Статус предмета: Обавезни			
Број ЕСПБ: 5			
Услов: Нема формалног услова			
Циљ предмета Обезбедити студенту дубоко разумевање принципа контроле и управљања безбедношћу информација и инфраструктура. Оспособити студента за обезбеђивање сигурности система применом административних, техничких и других безбедносних контрола, истовремено осигуравајући компатибилност са широким спектром поузданих оквира за информациону сигурност и захтевима за усаглашеност.			
Исход предмета Студент уме да идентификује и оцени ризике по безбедност информација и система. Уме да примени концепте управљања ризицима и стандарде, као и различите контролне оквире.			
Садржај предмета <i>Теоријска настава</i> <i>Управљање безбедношћу и ризицима.</i> Индустрија сајбер безбедности. Принципи информационе безбедности (Security governance principles - The confidentiality, integrity and availability of information; (CIA)). Управљање информационом/сајбер безбедношћу. Врсте информација и њихова класификација. Стратегија, политике и организација информационе/сајбер безбедности. Управљање ризицима (Security Risk Managment & Risk-based management concepts). Развој политика и процедура. <i>Усклађеност са регулативама и стандардима.</i> Контролни оквир (Security Governance Control Framework) и упознавање са контролним оквирима најбоље праксе (COBIT, CIS Controls, NIST Cybesecurity Controls (CSF), MITRE ATT&CK Framework и сл.). Мерење нивоа безбедности (Security Metrics) и извештавање. Legal and regulatory issues relating to information security; Међународни стандарди и регулатива (ISO, NIS2, CyberSecurity Act, GDPR, PCI-DSS, DORA, SWIFT, SOC Type1&2 Reporting). Безбедност информација и законски оквири у Србији. <i>Безбедносна култура и етика.</i> Безбедносна култура и управљање људским ресурсима (Security-first Culture & Human Resource Security). Родна разноврсност и инклузивност. Етика. Каријерни путеви у домену информационе безбедности. <i>Практична настава</i> Креирање безбедносних оквира за задату организацију. Тестирање/ревизија управљања сигурношћу за задату организацију.			
Литература 1. Security Engineering: A Guide to Building Dependable Distributed Systems, Ross J. Anderson, Wiley (2020) 2. CISM Certified Information Security Manager All-in-One Exam Guide, Peter H. Gregory, McGraw-Hill Education (2018)			
Број часова активне наставе		Теоријска настава: 25	Практична настава: 15
Методе извођења наставе Настава се изводи on-line коришћењем ZOOM или Microsoft Teams платформе.			
Оцена знања (максимални број поена 100)			
Предиспитне обавезе	поена	Завршни испит	поена
Кратки тестови	10 (10 x 1 поен)	усмени испит	30
Практични задаци	60 (5 x 12 поена)		



Студијски програм: КП Сајбер безбедност			
Назив предмета: ОДБРАМБЕНЕ БЕЗБЕДНОСНЕ ОПЕРАЦИЈЕ			
Наставник/наставници: Игор К. Франц , Владан З. Тодоровић , Тијана И. Героски			
Статус предмета: Обавезни			
Број ЕСПБ: 5			
Услов: Положени предмети Основе безбедности оперативних система и мрежа, Увод у развој и безбедност веб апликација, Принципи сајбер безбедности			
Циљ предмета			
Циљ предмета је да пружи дубоко разумевање одбрамбених методологија, принципа и алата безбедносног инжењеринга и анализе, као и да га оспособи за њихову практичну примену у реалним системима.			
Исход предмета			
Студент је способан да спроводи активности надгледања безбедносног стања организације, управља инцидентима током сајбер напада и обезбеђује континуитет у раду ИКТ система. Студент је способан да учествује у развоју, поставља и управља безбедносним решењима за инфраструктуре и производе.			
Садржај предмета			
Теоријска настава			
Логови и надгледање активности. Типови логова (системски, мрежни, апликативни). Анализа логова. Идентитети и одговорности. Обезбеђивање ресурса. Основни концепти безбедносних операција. Безбедносни оперативни центри (Security Operations Center - SOC). Технике обезбеђивања ресурса. Управљање инцидентима. Процес реаговања на инциденте. Опоравак од катастрофа. Управљање физичком безбедношћу. Континуитет пословања.			
Практична настава			
Безбедносни инжењеринг. Модел безбедности: дубинска одбрана, Zero trust оквир. Безбедносне праксе (network security, endpoint security, e-mail security, web security, web application firewall). Основе криптографије. Управљање идентитетима и дозволама за приступ: аутентификација, ауторизација, вишефакторска аутентификација (MFA/2FA), single sign-on, управљање привилегованим идентитетима. IAAA оквир. Основе безбедности окружења у облаку. Контрола рањивости сервера, софтвера и endpoint-a.			
Безбедносна анализа. Прикупљање и анализа податка (security/audit логова, логова мрежног саобраћаја, threat intelligence feeds, dark web). Алати безбедносних оперативних центара (Security Operations Center - SOC): SIEM, SOAR, EDR, XDR. Основе Cyber Kill Chain-a и MITRE ATT&CK оквира. Тријажа безбедносних инцидената. Аутоматизација одговора на инциденте.			
Литература			
1. Security Operations Center - Building, Operating, and Maintaining your SOC, Joseph Muniz, Gary McIntyre, Nadhem AlFardan, Cisco Press (2015)			
2. Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder, Don Murdoch GSE, Independently published (2014)			
Број часова активне наставе		Теоријска настава: 15	
		Практична настава: 30	
Методе извођења наставе			
Настава се изводи on-line коришћењем ZOOM или Microsoft Teams платформе.			
Оцена знања (максимални број поена 100)			
Предиспитне обавезе		поена	Завршни испит
Кратки тестови		10 (10 x 1 поен)	поена
		усмени испит	30
Практични задаци		60 (5 x 12 поена)	



Студијски програм: КП Сајбер безбедност			
Назив предмета: ОФАНЗИВНЕ БЕЗБЕДНОСНЕ ОПЕРАЦИЈЕ			
Наставник/наставници: Милош Р. Ивановић, Бранко М. Џакула, Дамјан М. Цветановић			
Статус предмета: Обавезни			
Број ЕСПБ: 5			
Услов: Положени предмети Основе безбедности оперативних система и мрежа, Увод у развој и безбедност веб апликација, Принципи сајбер безбедности			
Циљ предмета			
Циљ предмета је да пружи дубоко разумевање офанзивних тактика и методологија које користе етички хакери и тестери пенетрације, да студенту омогући разумевање хакерског начина размишљања, овладавање техникама тестирања пенетрације, анализе рањивости, идентификације рањивости у софтверу, мрежама и апликацијама, овладавање алатима за етичко хаковање, процену и ублажавање ризика, спремност на континуирано учење и прилагођавање.			
Исход предмета			
Студент је способан да процени ефективност безбедносних контрола, открива и искоришћава рањивости са циљем процене критичности у случају реалних напада.			
Садржај предмета			
Теоријска настава			
Третман и управљање рањивостима. Процена рањивости. Алати и технике за процену безбедности. Процес и циљеви процене безбедности. Тестирање одговора на инцидент. Тестирање могућности упада. Тестирање безбедности веб апликација. Безбедносно тестирање API-а. Тестирање рањивости софтвера. Алати за офанзивне безбедносне операције. Ревизија безбедности према стандардима.			
Практична настава			
Концепт црвених тимова (Red Teaming). Тестирање могућности упада (Penetration Testing). Офанзивни безбедносни инжењеринг. Open Source Intelligence (OSINT), Phishing и Hacking. Основе безбедности веб апликација. Основне врсте напада у веб апликацијама. OWASP Top 10 ranjivosti Web апликација. Увод у безбедносно тестирање веб апликација. Енумерација, XSS, IDOR, SSRF, удаљено извршавање кода, Безбедни циклус развоја софтвера.			
Литература			
1. Dafydd Stuttard, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Marcus Pinto, Wiley (2020)			
2. Red Team Field Manual, Ben Clark, Createspace Independent Publishing Platform (2014)			
Број часова активне наставе		Теоријска настава: 15	Практична настава: 30
Методе извођења наставе			
Настава се изводи on-line коришћењем ZOOM или Microsoft Teams платформе.			
Оцена знања (максимални број поена 100)			
Предиспитне обавезе		поена	Завршни испит
Кратки тестови		10 (10 x 1 поен)	усмени испит
Практични задаци		60 (5 x 12 поена)	30



Назив КП студија: Сајбер безбедност	
Врста и ниво студија: КП студија	
Наставник или наставници задужени за организацију стручне праксе : Ана М. Капларевић Малишић и Милош Р. Ивановић	
Број ЕСПБ: 5	
Услов: у складу са Законом о високом образовању и Статутом школе.	
Циљ Стицање практичних искустава током боравка студента у предузећима или другим радним срединама уз препознавање основних функција пословног, производног и технолошког система у домену сајбер безбедности.	
Очекивани исходи Стицање практичних искустава о раду и функционисању предузећа и радних средина окренута делатностима везаних за проучавање области. Да се студент оспособи за рад у одговарајућој специјализацији у оквиру предузећа у којима се реализује стручна пракса.	
Садржај стручне праксе Предмет се реализује кроз практични и самостални рад студента. Практичан рад подразумева боравак и рад у предузећима, установама и радним срединама у којима се обављају различите делатности повезане са специјалистичком оријентацијом. Избор тематске целине и привредног предузећа или друге организације спроводи се у консултацији са предметним професором. Током праксе студенти морају водити дневник у коме ће уносити опис послова које обављају, закључке и запажања. Након обављене праксе студенти праве извештај у форми семинарског рада са задатом темом који бране пред предметним наставником.	
Број часова , ако је специфицирано	90
Методе извођења Визуелно,запажања, самостални практичан рад,израда семинарског рада	
Оцена знања (максимални број поена 100)	
Активност у току предавања 0-60	
Одбрана семинарског рада 0-40	
Максимална дужна 1 страница А4 формата	
Ако у студијском програму постоји стручна пракса тада је обавезно дати описе који се траже	