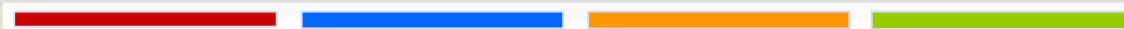


Заштита рачунарских система и мрежа



Садржај

- Увод
- Наставници
- Циљеви и исход предмета
- Програм предмета
- Лабораторијске вежбе
- Семинарски рад
- Финални практични тест
- Предиспитне обавезе студената
- Начин полагања испита
- Литература

Увод

- Назив предмета: Заштита рачунарских система и мрежа
- Година: 1, семестар: 2
- Фонд часова: 2 + 2 + 1
- Број ЕСПБ бодова: 6
- Предуслов: одслушани предмети Заштита података, Оперативни системи, Рачунарске мреже

Наставници

- **Предавања: др Павле Вулетих**
pavle.vuletic@etf.bg.ac.rs
Консултације после наставе и по договору
- **Предавања: др Жарко Станисављевић**
zarko@etf.rs
Консултације после наставе и по договору

Циљ предмета

- Упознавање студената са облашћу превенције упада у рачунарске системе и мреже. Обука студената за обављање послова из области заштите рачунарских система и мрежа и етичког упада у системе. Разумевање претњи и вектора напада на рачунарске и софтверске системе. Практичан рад студената на већем броју алата за анализу и детекцију напада.

Исход предмета

- Очекује се да студент који заврши овај курс може да:
 - разуме и познаје методологију упада у рачунарске системе и мреже
 - познаје различите врсте напада на рачунарске системе и мреже
 - активно користи већи број алата за детекцију и анализу претњи и напада на рачунарске системе и мреже
 - изврши етичке упаде у рачунарске системе и мреже као методу анализе рањивости.

Програм предмета

- Методологија и фазе упада у рачунарске системе и мреже. Извиђање, скенирање, прикупљање података. Физичка сигурност. Социјални инжењеринг. IP, ARP, DNS напади, BGP напади, DoS напади и ботнетови. Малвер, откривање лозинки, SQLi, XSS, слабости оперативних система. Приступне листе, firewall, алати за детекцију и превенцију упада, honeypot. Tor. Мобилна сигурност. Веб преваре. Етичко хаковање.

Лабораторијске вежбе

- Већи број лабораторијских вежби уз удаљени приступ (у било које време у дефинисаним временским периодима, могуће од куће).
- Лабораторијске вежбе **20 поена**
- Преглед вежби:
 - google searching, wireshark i nmap
 - ARP spoofing
 - DNS spoofing
 - firewall i access liste
 - SQLi
 - XSS
- **Важе годину дана**
- **Нема надокнаде**

Лабораторијске вежбе - окружење

- Лабораторије су подељене у три сегмента
- На крају сваког сегмента лабораторије тест преко Moodle платформе у вези са вежбама из тог сегмента.
 - Сегмент 1: Извиђање, прикупљање података, анализа пакета, мрежни напади (ARP spoofing, DNS spoofing)
 - Сегмент 2: firewall i access liste
 - Сегмент 3: SQL injection, XSS
- Лабораторија се ради самостално од куће или из рачунарских учионица на факултету. За сваку лабораторијску вежбу студенти ће се добити приступ одређеном броју виртуелних машина током неког временског периода.
- Тест се полаже у рачунарским учионицама на факултету.

Семинарски рад

- Носи **20 поена**
- **Нема надокнаде**
- **Важи годину дана**
- Одабрати један рад са BlackHat конференције из 2019. године
- Написати кратак извештај на максимално 3 стране
- Презентација+питања мах. 10 минута (уочи испита у јунском року)
- Сваки студент ће имати различиту тему. Списак одабраних тема ће бити објављен на Moodle курсу

Финални практични тест

- Носи **20** поена
- **Нема надокнаде**
- **Важи годину дана**
- Изазов (слично *Capture the Flag* изазовима) - открити слабост у систему, експлоатисати је и доћи до заштићене информације
- Термин: уочи испита у јунском року.

Предиспитне обавезе студената

- **Лабораторијске вежбе**
 - укупно 20 поена
 - Важи за текућу школску годину
- **Семинарски рад**
 - укупно 20 поена
 - Важи за текућу школску годину
- **Финални практични тест**
 - укупно 20 поена
 - Важи за текућу школску годину
- **Присуство настави**
 - Не оцењује се

Начин полагања испита

- Испит – 40 поена
 - Градиво са предавања

Начин полагања испита

Коначна оцена се формира на основу броја бодова на следећи начин:

- $91 \leq X < 100$ – оцена 10
- $81 \leq X < 91$ – оцена 9
- $71 \leq X < 81$ – оцена 8
- $61 \leq X < 71$ – оцена 7
- $51 \leq X < 61$ – оцена 6
- $0 \leq X < 51$ – студент није положио испит

Литература

- Материјали за предавања
- Материјали за вежбе

Листа

- Аутоматско пријављивање
- Обавештења иду на листу
- Поставити прослеђивање на адресу коју пратите

ОБАВЕШТЕЊЕ ЗА СТУДЕНТЕ

- Настава на предмету Заштита рачунарских система и мрежа подразумева изучавање различитих механизма којима се нарушава информациона безбедност и врше упади у рачунарске системе и мреже.
- Примена ових механизма када се извршавају према системима физичких и правних лица која нису упозната и сагласна са активностима на провери рањивости и тестирању упада у њихове системе је кажњива према Кривичном закону Републике Србије (Чланови 298 до 304а).
- Студенти на предмету Заштита рачунарских система и мрежа могу ове методе за потребе изучавања да користе искључиво у оквиру затвореног лабораторијског окружења које је обезбеђено за наставу на предмету Заштита рачунарских система и мрежа.
- Студенти не могу да подразумевају да су на било који начин охрабрени од стране наставника или да им се препоручује да користе ове методе који се изучавају према другим системима Електротехничког факултета или системима било ког трећег правног или физичког лица.
- Свака евентуална активност коју би предузео неки студент коришћењем ових метода и механизма према системима који нису у оквиру лабораторије на предмету искључива је одговорност студента.

Питања?

Електротехнички Факултет
Универзитет у Београду