Заштита рачунарских система и мрежа

Садржај

Увод

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

Наставници

- **Предавања: др Павле Вулетић**
  pavle.vuletic@etf.bg.ac.rs
  Часови online путем Zoom платформе снимани у термину предавања

  Консултације после наставе и по договору
- **Предавања: др Жарко Станисављевић**
  zarko@etf.rs
  Снимци часова доступни путем Moodle курса

  Консултације сваке недеље када има часова путем Zoom платформе

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 од куће (у било које време у дефинисаним временским периодима).
- Преглед вежби:
  - google searching, wireshark i nmap
  - ARP spoofing
  - DNS spoofing
  - firewall i access liste
  - Windows password hacking
  - Ескалација привилегија – buffer overflow напади
  - SQLi
  - XSS
- **Не оцењују се**
- **Припрема за финални практични тест**

Лабораторијске вежбе - окружење

- Лабораторије су подељене у четири сегмента
  - Сегмент 1: Извиђање, прикупљање података, анализа пакета, мрежни напади (ARP spoofing, DNS spoofing)
  - Сегмент 2: firewall i access liste
  - Сегмент 3: Windows password hacking и Ескалација привилегија
  - Сегмент 4: SQL injection, XSS
- Лабораторија се ради самостално од куће. За сваку лабораторијску вежбу студенти ће се добити приступ одређеном броју виртуелних машина током неког временског периода (зависи од броја студената на курсу).
- Два студента деле једно лабораторијско окружење

Семинарски рад

- Носи **20 поена**
- **Нема надокнаде**
- **Важи годину дана**
- Одабрати један рад са BlackHat конференције из 2020. или 2021. године
- Написати кратак извештај на максимално 3 стране
- Презентација+питања мах. 10 минута (уочи испита у јануарском року или у терминима током семестра)
- Сваки студент ће имати различиту тему. Списак одабраних тема ће бити објављен на Moodle курсу

Финални практични тест

- Носи **40 поена**
- **Нема надокнаде**
- **Важи годину дана**
- Изазов (слично *Capture the Flag* изазовима) - открити слабост у систему, експлоатисати је и доћи до заштићене информације
- Задаци на практичном испиту се састоје од елемената увежбаних на лабораторијским вежбама
- Термин: уочи испита у јануарском и јулском року.

Предиспитне обавезе студената

- **Лабораторијске вежбе**
  - Не оцењују се, али су припрема за финални практични тест
- **Семинарски рад**
  - укупно 20 поена
  - Важи за текућу школску годину
- **Финални практични тест**
  - укупно 40 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 <= X < 100 – оцена 10
- 81 <= X < 91 – оцена 9
- 71 <= X < 81 – оцена 8
- 61 <= X < 71 – оцена 7
- 51 <= X < 61 – оцена 6
- 0 <= X < 51 – студент није положио испит

Литература

- Материјали за предавања
- Материјали за вежбе

Комуникација

- Сајт предмета: https://rti.etf.bg.ac.rs/rti/ms1zrm/
- Moodle курс: https://elearning.rcub.bg.ac.rs/moodle/course/view.php?id=1152
- Мејл листа предмета: https://lists.etf.bg.ac.rs/wws/info/13m111zrm

ОБАВЕШТЕЊЕ ЗА СТУДЕНТЕ

- Настава на предмету Заштита рачунарских система и мрежа подразумева изучавање различитих механизама којима се нарушава информациона безбедност и врше упади у рачунарске системе и мреже.
- Примена ових механизама 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 законику 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 механизама према системима који нису у оквиру лабораторије на предмету искључива је одговорност студента.

Питања?

Електротехнички Факултет

Универзитет у Београду