Софийски университет "Св. Климент Охридски"

Факултет по математика и информатика

Одит на информационна сигурност

Сертификационнен курс на Асоциация за информационна сигурност – ISECA.org

Анотация:

Курсът "Одит на информационна сигурност" е предназначен за студенти и магистри във ФМИ на СУ, които имат желание да придобият или обогатят познанията си по информационна сигурност по отношение на разработка, инсталиране, конфигуриране, поддържка, управление и одитиране на информационни системи.
Курсът е с изключително практическа насоченост. Ще се разглеждат и използват програми за откриване на уязвимости, разработката на нови и модифициране на съществуващи. Включва запознаване с и преминаване през всички основни фази на техническия одит на софтуерни и мрежови компоненти, като:

- Изготвяне на план на одит за съответната компонента
- Изпълнение на плана
- Изготвяне на репорт
- Анализиране и обобщаване на резултати от цялостния одит.

Изисквания към студентите:

- Основни познания
  - на процеса по разработване на софтуер
  - на компютърни мрежи
  - по организация и работа на Интернет
- Курсът е предназначен за всички специалности

Придобити умения:

След завършване на този курс студентите ще могат да изготвят и изпълняват план за одит, както и да обобщават и анализират получените резултати. Най-добре представилите се ще получат признат сертификат от Асоциацията за информационна сигурност и нейните партньори за успешно преминато обучение по Одит на софтуерна сигурност. Ще има възможност за участие в реални проекти в тази сфера.

Изпити и оценки:

Изпитът се състои от два теста и задължителен проект. Тестовете включват 30 въпроса върху предавания материал. Съгласно предвидената система за оценяване от един тест могат да се спечелят до 30 точки, а от двата теста общо - до 60 точки. Проектът е задължителен. Студентите имат възможност да избират между софтуерна разработка и писмена разработка по предварително зададена тема. Темите няма да бъдат преподавани на курса или ако са засегнати в презентациите, при изготвянето на проекта ще изискват допълнителна и по-подробна информация, относно поставения проблем.
Проектът носи 40 точки.

Точки	Оценка
50 – 59	Среден 3
60 – 69	Добър 4
70 – 79	Мн. добър 5
80 - 100	Отличен 6

Дни и часове на провеждане:

Всеки вторник и четвъртък в зала 325 на ФМИ от 19.00 до 21.00 часа

Учебна програма:

1. Въведение – Увод в информационната сигурност?

Дефинират се понятията уязвимост, информационен риск, хакер, кракер, както и чисто психологични аспекти на информационната сигурност.

1.1 Каква е целта на курса?
1.2 Какво е информационната сигурност?
1.3 Защо е нужна?
1.4 Какъв е смисълът да се правят одити?

2. Одит на физическата сигурност.

Представят се концептуалните изисквания към физическата сигурност и системите за наблюдение от гледна точка на стандартите по информационна.

2.1 Устройства за ограничаване на физическия достъп (ключалки).
2.2 Биометрични системи за достъп
2.3 Магнитни карти
2.4 Smart карти
2.5 RFID
2.6 Алармени системи, датчици и сензори за откриване на нарушители
2.7 Противопожарна защита
2.8 Атаки в/у физическа преносна среда

3. Одит на мрежовата сигурност (втори, трети и четвърти слой от OSI модела).

Разглеждат се основните протоколи на datalink слоя, пряко свързани с преносните си среди - PPP, ethernet, безжични мрежи (801.11), DOCSIS (по кабелни мрежи за пренос на телевизионен сигнал), VPN мрежи.

3.1 Проверки на datalink слоя
  3.1.1 Ethernet, VLAN изолация
  3.1.2 DOCSIS
  3.1.3 Wireless мрежи (802.11*)
3.2 Проверки на network и transport слоя
  3.2.1 Firewalls
  3.2.2 Нужни/ненужни услуги
  3.2.3 Routing и routing протоколи
  3.2.4 VPN

4. Одит на сигурността на операционните системи.

Разглеждат се основните принципи по организация на работата на операционните системи, след което се анализират изискванията и потенциалните проблеми по отношение на сигурността при Microsoft и UNIX базирани операционни системи.

4.1 Trusted операционни системи
4.2 UNIX базирани
4.3 Microsoft базирани
4.4 Security updates
4.5 Автоматизирани инструменти

5. Одит на сигурността на софтуер.

5.1 Автоматизирани инструменти
5.2 Анализ на изходния код
5.3 Анализ на бинарния код
5.4 Основни принципи при разработката на exploit-и

6. Одит на сигурността на web услуги и приложения

Специално внимание се отделя на web базираните приложения.

6.1 XSS

6.2 Различни видове injections
6.3 Автоматизирани инструменти

7. Одит на сигурността на цялостни системи
7.1 authentication и authorization
7.2 отдалечено администриране и достъп
7.3 change management
7.4 monitoring

8. Осми слой на OSI модела
8.1 Тестове за психологична устойчивост
8.2 Принципи и приложение на social engineering „похвата”

9. Разглеждане на стандарти за системи за управление на информационната сигурност (СУИС). ISO 17799:2003, ISO 27001:2005 (наследникът на ISO/BS 7799-2:2002)
9.1 История на стадартите
9.2 Идея
9.3 Достъпност
9.4 Приложение
9.5 Описание

10. Стандарти за одитиране и информационна сигурност на US DoD.
10.1 История на стадартите
10.2 Идея
10.3 Достъпност
10.4 Приложение
10.5 Описание

11. Провеждане на практически одит на сигурността на софтуерни и мрежови компоненти.
11.1 Направа на план за одитиране
11.1.1 Разработка на checklists
11.2 Пракическо одитиране
11.3 Анализ и изготвяне на доклад от одита на информационната сигурност

Първа сбирка:

За повече информация:

http://training.iseca.org/