КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ

ІМЕНІ БОРИСА ГРІНЧЕНКА

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

Затверджено на засіданні кафедри
інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
(протокол № 5 від 03.04.24)

РОБОЧА ПРОГРАМА ІСПИТУ

ПРИКЛАДНІ АСПЕКТИ ТЕСТУВАНЬ НА ПРОНИКНЕННЯ ТА ЕТИЧНОГО ХАКІНГУ

галузь знань	12 Інформаційні технології
спеціальність	125 Кібербезпека та захист інформації
освітня програма	125.00.01 Безпека інформаційних і комунікаційних систем

2023-2024 навчальний рік

Опис програми іспиту

Київський столичний університет імені Бориса Грінченка

Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

Програма іспиту з дисципліни
«Прикладні аспекти тестувань на проникнення та етичного хакінгу»

1 курс – освітній рівень – другий (магістерський)

Спеціальність 125 Кібербезпека та захист інформації

Освітня програма: 125.00.01 Безпека інформаційних і комунікаційних систем

Форма проведення: тестування на платформі Moodle в ЕНК дисципліни: https://elearning.kubg.edu.ua/course/view.php?id=21437

Тривалість проведення **1 год. 20 хв.**

Максимальна кількість балів: **40 балів**

Екзамен проводиться в університетській аудиторії у тестовій формі із використанням персональних комп'ютерів, якщо ситуація дозволяє проведення освітнього процесу офлайн. Якщо ж освітній процес проходить дистанційно, то екзамен проводиться онлайн в режимі відеоконференції засобами Google Meet.

Форма проведення екзамену – комбінована. Екзамен оцінюється у 40 балів за розподілом: 20 балів – комплексний комп'ютерний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання.

Критерії оцінювання практичного завдання (задачі):

20-17 балів: Відмінний рівень умінь, розв'язання задачі повне, вичерпне володіння програмним забезпеченням, можливими, незначними недоліками

16-13 балів: Добрий рівень умінь, розв'язання задачі містить небагато недоліків та / або незначну кількість помилок

12-9 балів: Мінімально допустимий рівень умінь, що характеризується недостатнім рівнем володіння програмним забезпеченням, розв'язання задачі неповне, містить недоліки та помилки

8-5 бали: Незадовільний рівень умінь, що виявляється у нездатності застосувати знання при розв'язанні задач.

4-1 бал: Незадовільний рівень умінь, що виявляється у неспроможності володіння програмним забезпеченням, невмінні розв'язувати задачі.

0 балів: Відповідь відсутня.

Екзамен проводиться із суворим дотриманням принципів академічної доброчесності, що передбачає недопустимість списування, фальсифікацій та обману. При порушенні студент відсторонюється від подальшого проходження екзаменаційного тесту із підсумковою оцінкою Fx за дисципліну. При виконанні завдань допускається користування довідковою літературою, таблицями значень функції, критеріїв та ін.

Підсумкова оцінка в балах (максимально 100 балів) за дисципліну є сумою результату поточного контролю за семестр (60 балів) та відповіді на екзамені (40 балів).

Перелік тем, які виносяться на іспит:

1. Основні терміни тестування на проникнення.
2. Хто такі хакери та етичні хакери?
3. Що роблять справжні хакери?
4. Методології тестування на проникнення: OSTMM та ISSAF.
5. Управління проектами проникнення.
6. Огляд інструментів злому.
7. Законодавча база в галузі хакінгу.
8. Методи відкритої розвідки.
9. Огляд структурованих аналітичних методів.
10. Типи інформації.
11. Виявлення джерел інформації.
12. Принципи роботи пошукових ботів.
13. Оператори розширеного пошуку Google.
14. Виявлення IP-адрес.
15. Трасування маршрутів.
16. Використання Maltego.
17. Використання theHarvester.
18. Підміна зони DNS.
19. Примусове використання DNS.
20. Типи вразливостей.
21. Пошук уразливостей вручну.
22. Автоматизований пошук уразливостей.
23. Інструменти аналізу вразливостей.
24. Використовувати бази даних паролів для підбору.
25. Google для тестів на проникнення.
26. Локальні та віддалені експлойти.
27. Особливості фреймворка Metasploit.
28. Атака людина по середині.
29. Онлайн і офлайн атаки на паролі.
30. Ручний підбір паролів.
31. Проведення атаки на хеші.
32. Робота з третіми особами.
33. Визначення соціальної інженерії.
34. Типова структура веб-додатків.
35. Загальні веб-уразливості.
36. Проекти OWASP.
37. Огляд фреймворка з тестування OWASP.
38. Google Hacking Database (GHDB).
39. Засоби тестування веб-безпеки.
40. Підтримка методів доступу.
41. Використання Meterpreter.
42. Етичний злом.
43. Kali Linux.
44. Сканери портів.
45. Сканери вразливостей.
46. Які є юридичні особливості для проведення досліджень з безпеки інформації?
47. Як формується експерименту в сфері кібернетичної безпеки?

48. Які існують обмеження для експериментальних розробок в сфері пошуку вразливостей інформаційних систем?
49. Наведіть приклади захищеного віртуального середовища для проведення експериментів з безпеки інформації.
50. Яке завдання з кібернетичної безпеки поставлено в вашій науковій роботі?
51. Як правильно поставити експеримент у сфері кібернетичної безпеки?

Екзаменатор  Володимир СОКОЛОВ

Завідувач кафедри  Павло СКЛАДАННИЙ