АСПЕКТИ ТЕСТУВАНЬ НА ПРОНИКНЕННЯ ТА ЕТИЧНИЙ ХАКІНГ

Тип дисципліни	Вибіркова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Кількість встановлених кредитів ЄКТС	8,0
Форми навчання, для яких викладається дисципліна	Денна

Результати навчання
Студент, який успішно завершив вивчення дисципліни, повинен:
знати загальні терміни етичного хакерства: уразливості, експлуатація, корисне навантаження, нульовий день; методологію тестування проникнення; використання спільних уразливостей; здійснення атак на паролі; здійснення атак «людина по середині»; роботу сканерів вразливостей;
вміти використовувати інструменти для етичного злому; готувати звіт із висновками та рекомендаціями щодо рівня захищеності інформаційно-комунікаційних систем;
володіти практичними навичками проведення аудиту безпеки інформаційно-комунікаційних систем.

Зміст навчальної дисципліни. Основні терміни тестування на проникнення. Методології тестування на проникнення: OSTMM та ISSAF. Управління проектами проникнення. Огляд інструментів злому. Законодавча база в галузі хакінгу. Методи відкритої розвідки. Огляд структурованих аналітичних методів. Типи інформації. Виявлення джерел інформації. Принципи роботи пошукових ботів. Оператори розширеного пошуку Google. Виявлення IP-адрес. Трасування маршрутів. Використання Maltego. Використання theHarvester. Підміна зони DNS. Примусове використання DNS. Типи вразливостей. Пошук уразливостей вручну. Автоматизований пошук уразливостей. Інструменти аналізу вразливостей. Google для тестів на проникнення. Локальні та віддалені експлойти. Особливості фреймворка Metasploit. Атака людина по середині. Онлайн і офлайн атаки на паролі. Ручний підбір паролів. Проведення атаки на хеші. Робота з третіми особами. Соціальна інженерія. Google Hacking Database (GHDB). Засоби тестування веб-безпеки. Підтримка методів доступу. Використання Meterpreter. Етичний злом. Сканери портів. Сканери вразливостей.

Запланована навчальна діяльність: кількість аудиторних годин - не менше 1/3 від загальної кількості годин, які заплановані для вивчення дисципліни.

Форми (методи) навчання: лекції (з використанням методів проблемного навчання і візуалізації); лабораторні заняття (з використанням методів комп'ютерного моделювання, тренінгів, майстер-класів), самостійна робота (індивідуальні завдання), використання сучасних інформаційних технологій та прикладного програмного забезпечення.

Форми оцінювання результатів навчання: усне опитування, захист лабораторних робіт, письмова контрольна робота.

Вид семестрового контролю: залік

Навчальні ресурси:
1. Ethical Hacking and Penetration Testing Guide/ Rafay Baloch. - Auerbach Publications, 2014. – 531 p.
2. Georgia Weidman. Penetration testing. A Hands-On Introduction to Hacking/ Georgia Weidman. – San Francisco, 2014. – 531 p.
3. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khnu.km.ua.
4. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Викладачі: к.т.н., доц. Тітова В.Ю.