Анотація до навчальної дисципліни

ОСНОВИ ЕТИЧНОГО ХАКІНГУ

Метою викладання дисципліни «Основи етичного хакінгу» - надати студентам знання, необхідні для оцінки вразливостей інформаційних систем та напрацювання рекомендацій щодо стратегій їх пом'якшення, та навички етичного хакера.

Завданням дисципліни є – надати студентам широкі практичні навички в галузі наступальної безпеки, які дозволять завчасно виявити невідомі загрозі та усунути їх раніше, ніж ними скористаються зловмисники. Навчити стулентів розумінню мислення кіберзлочинців, тактики загроз під час впровадження засобів контролю безпеки та моніторингу, реагування на поточні загрози безпеці.

Надати навичок, необхідних для працевлаштування у сферах, пов'язаних із кібербезпекою, на посадах, які вимагають комплексної підготовки у галузях комп'ютерних мереж, кібербезпеки та програмування. Ці навички отримуються на вирішенні практичних завдань з реального світу кібербезпеки.

Вивчення курсу передбачає теоретичну підготовку і практичне вивчення матеріалу з використанням персональних комп'ютерів, програмного забезпечення для моделювання мереж Packet Tracer, VM лабораторного середовища.

При розробці курсу використовувалися матеріали мережної академії Cisco, а саме курсу: Ethical Hacker. За умови успішного вивчення курсу студенти додатково отримають сертифікати та цифрові бейджі про успішне завершення курсу Академії Cisco Ethical Hacker.

В результаті вивчення навчальної дисципліни студент повинен
знати:

- пояснювати важливість етичного хакерства та тестування на проникнення;
- описувати різні методології та фреймворки тестування на проникнення;
- пояснювати, як атаки соціальної інженерії досягають успіху;
- пояснювати, як інструменти соціальної інженерії сприяють атакам;
- пояснювати, як використовувати вразливості мереж, дротового та бездротового зв'язку;
- пояснювати типові атаки на веб-застосунки;
- пояснювати clickjacking;
- пояснювати як використовуються вразливості на основі авторизації;
- пояснювати вразливості cross-site scripting;

- пояснювати cross-site request forgery (CSRF/XSRF) атаки;
- пояснювати як використовуються вразливості незахищеного коду;
- пояснювати як використовуються вразливі місця в безпеці хмари, мобільних пристроїв і Інтернету речей;
- пояснювати які роботи потрібно виконати після експлуатації вразливості з метою запобігання такої практики в майбутньому;
- пояснювати необхідні складові спілкування під час проведення тесту на проникнення.

вміти:

- налаштовувати віртуальну машину для виконання навчальних вправ з тестування на проникнення;
- створювати тести на проникнення, планувати їх документальну підтримку;
- виконувати дії зі збору інформації та сканування вразливостей;
- виконувати пасивну розвідувальну діяльність;
- проводити активну розвідувальну діяльність;
- виконувати сканування вразливостей;
- аналізувати результати сканування вразливостей;
- створювати звіти про тестування на проникнення;
- рекомендувати організації відповідні виправлення на основі результатів тесту на проникнення;
- класифікувати інструменти тестування на проникнення за основними сферами використання.

Структура навчальної дисципліни " Основи етичного хакінгу"

Тема 1: Вступ до етичного хакерства та тестування на проникнення

Тема 2: Планування та визначення обсягу тестування на проникнення

Тема 3: Збір інформації та сканування вразливостей

Тема 4: Атаки соціальної інженерії

Тема 5: Злам дротових і бездротових мереж

Тема 6: Експлуатація вразливостей програмного забезпечення

Тема 7: Безпека хмарних обчислень, мобільних застосунків та Інтернету речей

Тема 8: Дії після зламу. Звітність та комунікація

Тема 9: Аналіз інструментів тестування на проникнення