Итоговая аттестация
по дополнительной общеобразовательной общеразвивающей программе «Этичный хакинг на Python: The Art of Exploitation»

Место итоговой аттестации в программе: по итогам прохождения четырех модулей Программы

Количество академических часов: 4 ак.ч.

Форма контроля: защита итогового проекта (индивидуального или группового) «Разработка системы обнаружения и предотвращения атак на веб-приложение»

Учащимся предлагается разработать системы обнаружения и предотвращения атак на веб-приложении.

Защита итогового проекта: подготовка и защита итогового проекта может быть выполнена как индивидуально, так и группой учащихся.

Количество прохождения итоговой аттестации (защиты игрового творческого проекта) не ограничено.

Процедура оценивания итогового проекта

Оценка итогового проекта осуществляется в соответствии с системой критериев. Каждый критерий оценивается по следующим рубрикаторам:

- не соответствует критерию (0 баллов)
- скорее соответствует, чем не соответствует критерию (1 балл)
- скорее соответствует, чем не соответствует критерию (2 балла)
- полностью соответствует критерию (3 балла)

Максимально возможное количество баллов за итоговый проект: 30 баллов

В рамках процедуры оценивания технические баллы переводятся в следующую шкалу оценки: от 0% до 50% (0-15 баллов) – не зачтено и от 51% до 100% (16-30 баллов) – зачтено.

Критерии оценивания итогового проекта

1. Владение технологиями показано на уровне реализаций проектов подобных типов
2. Проект выполнен в соответствии с современными подходами в заявленной тематической области
3. Проект выполнен самостоятельно, без содержательной помощи преподавателя
4. В проекте корректно используется язык программирования Python
5. Требования к стилю кода соблюдены
6. Графические элементы интерфейса отображаются корректно, текстовые элементы не содержат языковых ошибок
7. Используются оптимальные алгоритмы и структура базы данных, а также оптимальные запросы к базе данных
8. Терминология соответствует решаемой проблеме и используется правильно
9. Интерфейс интуитивно понятен пользователям, удобен в использовании
10. Проект выполнен и представлен на проверку с соблюдением дедлайна

Задание для итогового проекта
«Разработка системы обнаружения и предотвращения атак на веб-приложение»

Описание проекта: необходимо разработать систему, способную обнаруживать и предотвращать атаки на веб-приложение. В выполнении каждого из этапов проекта вам понадобятся знания и умения, которые вы освоили в рамках нашего курса.

Проект может быть выполнен как индивидуально, так и коллективно. Если проект выполняется группой учащихся, тогда команде предстоит совместно разработать защищенную систему, которая будет способна обнаруживать и предотвращать различные атаки на веб-приложение. Для эффективной работы нужно будет распределить между членами команды задачи каждого этапа проекта (отдельные его пункты). Это ускорит написание общей итоговой программы и обеспечит более высокое качество проекта.

Этапы реализации проекта

ЭТАП 1

1. Напишите эффективные алгоритмы для обработки данных веб-приложения, используя продвинутые функции и структуры данных на Python (вы изучали это в теме 1.1. Обзор продвинутых возможностей Python).
2. Разработайте модуль для сохранения и загрузки данных веб-приложения в базу данных, учитывая безопасность и защиту от SQL-инъекций. Создайте файловое хранилище для логирования событий и записи результатов анализа атак на веб-приложение (вы изучали это в теме 1.2. Работа с файлами и базами данных).
3. Используйте многопоточность для обработки параллельных запросов к веб-приложению и анализа сетевого трафика в режиме реального времени (вы изучали это в теме 1.3. Многопоточное программирование и параллельные вычисления)
4. Создайте графический интерфейс, который будет обеспечивать удобное взаимодействие пользователя с системой обнаружения и предотвращения атак (вы изучали это в теме 1.4. Разработка интерфейсов с использованием графических библиотек).

ЭТАП 2

1. Проведите анализ уязвимостей в сетевых протоколах, используемых веб-приложением, и определите их потенциальные угрозы (вы изучали это в теме 2.1. Анализ уязвимостей в сетевых протоколах).
2. Разработайте методы перехвата и анализа сетевого трафика, направленного на веб-приложение, с целью обнаружения атак и аномалий (вы изучали это в теме 2.2. Продвинутые методы перехвата и анализа трафика).
3. Разработайте механизмы обнаружения и предотвращения сниффинга и ARP-атак на веб-приложение (вы изучали это в теме 2.3. Сниффинг и ARP-атаки).
4. Создайте систему защиты сетевых ресурсов веб-приложения, включая обнаружение и блокировку подозрительной активности и атак (вы изучали это в теме 2.4. Противодействие атакам и защита сетевых ресурсов).

ЭТАП 3

1. Изучите уязвимости веб-приложений и разработайте методы их эксплуатации с целью проверки защищенности системы (вы изучали это в теме 3.1. Уязвимости веб-приложений и их эксплуатация).
2. Разработайте механизмы защиты базы данных веб-приложения от SQL-инъекций и других атак, используя соответствующие методы и фильтры (вы изучали это в теме 3.2. SQL-инъекции и защита баз данных).

3. Разработайте методы обнаружения и предотвращения атак на сессии и механизмы аутентификации веб-приложения (вы изучали это в теме 3.3. Атаки на сессии и механизмы аутентификации).
4. Создайте систему защиты веб-приложения, включающую фильтрацию входящего трафика и обнаружение подозрительной активности (вы изучали это в теме 3.4. Защита веб-приложений и противодействие атакам).

ЭТАП 4

1. Разработайте методы сбора и анализа цифровых следов атак на веб-приложение для последующей экспертизы (вы изучали это в теме 4.1. Форензика и судебная экспертиза).
2. Разработайте методы обнаружения и предотвращения социальной инженерии и фишинга веб-приложения (вы изучали это в теме 4.2. Социальная инженерия и фишинг).
3. Исследуйте и анализируйте методы обхода защиты веб-приложения, а затем разработайте методы их обнаружения и предотвращения (вы изучали это в теме 4.3. Анализ и обход защиты системы).
4. Разработайте архитектуру безопасной системы для веб-приложения, включая механизмы защиты и мониторинга (вы изучали это в теме 4.4. Проектирование и реализация безопасных систем).

ЭТАП 5:

1. Подготовьте презентацию к защите итогового проекта, где вы продемонстрируете исходный код и работоспособность программы, которая будет способна обнаруживать и предотвращать различные атаки на веб-приложение.

2. Подготовьтесь к защите итогового проекта на итоговой аттестации, учитывая критерии оценивания проекта.