Всероссийская олимпиада школьников. Информатика.
Профиль Информационная безопасность.
Муниципальный этап.
Проектный тур. 9-11 классы.

Вам доступно на выбор одно из двух направлений: Red Team и Blue Team.

Red Team – направление исследования, доказательства и демонстрации уязвимостей и слабых мест в информационных системах, программном обеспечении или организационных процессах.

Blue Team – разработка решения, которое повышает общий уровень безопасности системы, упрощает работу аналитиков или автоматизирует рутинные операции по обеспечению ИБ.

Необходимо выбрать **одно** направление и ответить на соответствующие вопросы, которые относятся к нему.

Ответ на каждый вопрос – до 150 слов. Информация, указанная после 150-го слова, не учитывается в ответе.

Продолжительность тура – 2 ч 30 мин (150 мин).

Если проект нацелен на создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ст. 273 УК РФ), то он оценивается в 0 баллов.

Blue Team вопросы

1. Сформулируйте актуальную проблему информационной безопасности, которую решает ваш проект. Также укажите тактику/тактики согласно MITRE ATT&CK, от техник реализации которых обеспечивает защиту ваш продукт.

- Формулировка актуальной проблемы информационной безопасности (Сформулирована проблема информационной безопасности, актуальность аргументирована с приведением процессов или/и ситуаций, в которых она возникает — 3 балла; сформулирована актуальная проблема, но актуальность не аргументирована — 1 балл; проблема не сформулирована ИЛИ неактуальна — 0 баллов);

- Перечень тактик MITRE ATT&CK (Указаны две или более тактики MITRE ATT&CK, соответствующие сформулированной проблеме – 3 балла; указана одна тактика MITRE ATT&CK, соответствующая сформулированной проблеме – 1 балл; тактики не указаны ИЛИ не соответствуют сформулированной проблеме – 0 баллов).

2. Опишите идею разрабатываемого решения, сформулируйте цель и задачи проекта. Укажите предполагаемую форму реализации продукта (программа / программно-аппаратный комплекс / алгоритм / сервис / сайт /…).

- Описание идеи разрабатываемого решения (Сформулирована авторская концепция проекта, исчерпывающе описывающая предлагаемое решение и исключающая двусмысленное толкование – 2 балла; описание идеи не создает общего представления о реализуемом продукте – 0 балл);

- Формулировка цели и задач проекта (Указаны параметры успешной реализации проекта – 2 балла; сформулированные цель и задачи не позволяют оценить успешность реализации проекта – 0 балл);

- Описание предполагаемой формы реализации (Предполагаемая форма реализации продукта описана полно – 2 балла; описание вида продукта неполно – 1 балл; описание не позволяет оценить возможность внедрения продукта – 0 баллов).

Если описанная идея не решает указанную проблему информационной безопасности – 0 баллов за весь вопрос.

3. Укажите требования к функционалу и техническим характеристикам разрабатываемого продукта.

Корректен и полон список измеримых (количественных) и качественных требований к параметрам разрабатываемого продукта — 6 баллов; не описаны некоторые параметры или есть неточности в описании — 3 балла; по приведенному описанию невозможно оценить состоятельность разрабатываемого продукта или характеристики неадекватны — 0 баллов.

Если заявленный функционал не позволяет решить указанную проблему информационной безопасности – 0 баллов за весь вопрос.

4. Опишите алгоритм работы вашего решения с указанием используемых в нём технологий/алгоритмов/классов решений.

- Описание алгоритма (Продемонстрировано, как продуктом проекта будет достигнута возможность выполнения всех поставленных задач – 4 балла; приведено общее описание достижения функциональности продукта – 2 балла; обоснование функциональности продукта не описано и не является очевидным – 0 баллов);

- Соответствие выбранных технологий и инструментария описанному алгоритму (выбор технологий и инструментария рационален – 2 балла; выбраны не оптимальные технологии и инструментарий – 1 балл; использование выбранных технологий и инструментария не разумно – 0 баллов).

Если описанный алгоритм не решает указанную проблему информационной безопасности – 0 баллов за весь вопрос.

5. Опишите преимущества вашего решения в сравнении с существующими аналогами.

Проведён сравнительный анализ, описаны преимущества предлагаемого решения над всеми передовыми решениями в исследуемой сфере ИЛИ обосновано отсутствие решений указанной проблемы — 6 баллов; в сравнительном анализе не были рассмотрены некоторые популярные решения, но преимущество имеет место быть — 3 балла; анализ потенциальных аналогов отсутствует / проведён некачественно или продукт не обладает преимуществами над приведёнными аналогами — 0 баллов).

Если предложенное решение не решает указанную проблему информационной безопасности – 0 баллов за весь вопрос.

Red Team вопросы

1. Укажите уязвимость/уязвимости/класс уязвимостей/слабые места, на выявление, демонстрацию или описание которой(-ых/-ого) направлен ваш продукт, а также информационные системы, программном обеспечение или организационные процессы, для которых эта слабость в обеспечении информационной безопасности является актуальной.

- Актуальность (Успешная эксплуатация уязвимости/уязвимостей/класса уязвимостей/слабых мест влечет существенные потери (серьезные финансовые убытки/репутационные потери компании/несанкционированный доступ или утечка большого количества данных/доступ к объектам критической информационной инфраструктуры и др.) – 2 балла; последствия не являются критичными для рассматриваемой целевой информационной системы – 0 баллов);

- Новизна вектора атаки или подхода (Предложена ранее не описанная атака ИЛИ ранее не описанная уязвимость ИЛИ ранее не описанный подход к выявлению или демонстрации уязвимости – 2 балла; существенно доработана известная атака ИЛИ существенно доработан подход к выявлению или демонстрации известной уязвимости – 1 балл; рассмотрена широко известная атака ИЛИ широко известная уязвимость ИЛИ подход к выявлению/демонстрации уязвимости не является новым – 0 баллов);

- Масштаб охвата угроз (Продукт направлен на выявление или демонстрацию класса уязвимостей ИЛИ нескольких тактик атак согласно MITRE ATT&CK – 2 балла; продукт направлен на реализацию одной тактики атаки согласно MITRE ATT&CK – 1 балл; продукт направлен на выявление или демонстрацию единичной уязвимости – 0.5 балла; продукт не связан с выявлением/демонстрацией уязвимостей или реализацией атаки – 0 баллов).

2. Опишите концепцию разрабатываемого продукта, сформулируйте цель и задачи проекта. Укажите предполагаемую форму реализации продукта (программа / программно-аппаратный комплекс / алгоритм / сервис / сайт /…).

- Описание идеи разрабатываемого решения (Сформулирована авторская концепция проекта, исчерпывающе описывающая конечный продукт и исключающая двусмысленное толкование – 2 балла; описание идеи не создает общего представления о реализуемом продукте – 0 баллов);

- Формулировка цели и задач проекта (Указаны параметры успешной реализации проекта – 2 балла; сформулированные цель и задачи проекта не позволяют оценить успешность реализации проекта – 0 баллов);

- Описание предполагаемой формы реализации (Предполагаемая форма реализации продукта описана полно – 2 балла; описание вида продукта неполно – 1 балл; описание не позволяет оценить возможность использования продукта проекта – 0 баллов).

3. Для оценки автоматизации и воспроизводимости опишите принцип взаимодействия с вашим инструментом для выявления или демонстрации рассматриваемой(-ых/-ого) вами уязвимости/уязвимостей/класса уязвимостей/слабых мест. Укажите действия, которые необходимо воспроизвести пользователю для использования вашего инструмента, и условия, необходимые для его корректной работы.

- Полнота описания (Приведённое описание полно и чётко описывает действия пользователя – 2 балла; из приведённого описания не ясна последовательность действий пользователя инструмента, которая позволяет выявить или продемонстрировать уязвимость/уязвимости/класс уязвимостей/слабые места – 0 баллов);

- Степень автоматизации и воспроизводимости (Инструмент полностью автоматизирует процесс выявления или демонстрации рассматриваемой уязвимости - 4 балла; инструмент позволяет автоматизировать только часть действий, при этом существенную часть анализа уязвимости/воспроизведения атаки пользователь должен выполнять самостоятельно - 2 балла; продукт является набором рекомендаций/методическим документом и не позволяет автоматизировать процесс выявления или демонстрации (эксплуатации) рассматриваемой уязвимости или реализации рассматриваемой атаки - 0 баллов).

4. Опишите алгоритм разрабатываемого вами продукта с указанием используемых в нём технологий/алгоритмов/классов решений.

- Описание алгоритма (Продемонстрировано, как продуктом проекта будет достигнута возможность выполнения всех поставленных задач – 4 балла; приведено общее описание достижения функциональности продукта – 2 балла; обоснование функциональности продукта не описано и не является очевидным – 0 баллов);

- Архитектура и дизайн (Продемонстрирована модульность разрабатываемого алгоритма – 2 балла; не планируется использовать методы, позволяющие сделать алгоритм модульным и читаемым – 0 баллов).

5. Опишите результаты применения вашего продукта, на основе которых могут быть сформулированы рекомендации (меры) по устранению рассматриваемой(-ых/-ого) вами уязвимости/уязвимостей/класса уязвимостей/слабых мест в целевых информационных системах, программном обеспечении или организационных процессах.

(Формат представления результатов работы продукта позволяет идентифицировать местоположение, формат и детали уязвимости в тестируемой системе – 6 баллов; уязвимость описана точно, но не указывается в какой части тестируемой системы она находится ИЛИ указано местоположение, но нет точного описания уязвимости – 3 балла; представленные результаты не позволяют устранить рассматриваемую уязвимость – 0 баллов).