

**Практическое задание для регионального этапа всероссийской олимпиады
школьников по технологии 2024 – 2025 учебный год
Профиль “Информационная Безопасность”, 11 класс**

Тематики заданий

В туре необходимо решить как можно больше заданий. Наборы заданий ориентированы на комплексную оценку навыков участников заключительного тура и охватывают перечисленные ниже темы:

1. Реверс (анализ исходных текстов компьютерных программ)
2. Web (поиск уязвимостей web-приложений)
3. Forensics (поиск следов инцидентов информационной безопасности)
4. Linux\Unix (Misc) (задания смешанной категории, защита ОС Linux\Unix)
5. Анализ трафика
6. Средства защиты информации (СЗИ).

Примечания:

Оценка заданий (кроме тематики СЗИ) производится автоматически по факту размещения участником в поле для ввода корректного флага – строки определенного вида (шаблон будет озвучен перед началом тура), доступ к которому является индикатором успешного решения задания.

Оценка заданий по тематике СЗИ производится организаторами на основании предоставленных участниками файлов.

Максимально возможное число баллов за практический тур – 35 баллов.

Инструкция для участника приложена к данному документу (Приложение А).

Время на изучение инструкции (до 30 минут) не входит в общее время выполнения заданий.

Инструкция для администраторов распространяется отдельно, является конфиденциальной и участникам не предоставляется.

Инфраструктура участника

1. На ПК участника олимпиады должен отсутствовать доступ в сеть “Интернет”.
2. На ПК участника установлен гипервизор VirtualBox¹.
3. Участнику предоставляется образ виртуальной машины с необходимым программным обеспечением для решения заданий. Виртуальную машину участника требуется запустить до начала практического тура.
4. На сервере организаторов запускается виртуальная машина с Платформой с заданиями, которая используется для решения всех заданий, кроме заданий по работе с СЗИ. ***Развертывание Платформы для каждого класса производится непосредственного организаторами не позднее чем за 1 день до проведения практического тура.*** Виртуальная машина с Платформой также должна быть доступна по локальной сети с машин участников.
5. До начала выполнения заданий все участник должны быть зарегистрированы на Платформе STFd и получить логин/пароль.
6. Для загрузки участниками файлов (скриншотов, скриптов, конфигурационных файлов и т.п.), подтверждающих выполнение заданий тематики СЗИ, организаторы предоставят механизм индивидуальной загрузки этих файлов (индивидуальные папки с персональным доступом для каждого участника).

Порядок проведения

Длительность практического тура (выполнение практических заданий) для участников 11 класса составляет: **3 часа 30 минут** (без учета перерывов). В случае обнаружения неисправности в оборудовании, возникшей не по вине участника, по решению наблюдателя данный участник может пересест на резервный ПК. Время, затраченное на выявление и устранение такой неисправности, компенсируется.

Общие требования

1. До начала практического тура необходимо обеспечить доступ с ПК участников к Платформе с заданиями, развернутой на сервере. На экранах ПК участника должны быть выведены окна регистрации на платформе с заданиями.
2. После старта практического тура, участник должен выполнять задания полностью самостоятельно. Задания расположены на Платформе. Программный инструментарий для их решения доступен на виртуальных машинах на ПК участников.
3. По окончании решения заданий участник олимпиады может покинуть аудиторию.
4. Найденные флаги (кроме заданий СЗИ) вводятся на Платформе. Количество попыток ввода флага не ограничено. За ошибочно введенный флаг баллы не снижаются.

¹ <https://www.virtualbox.org/wiki/Downloads>

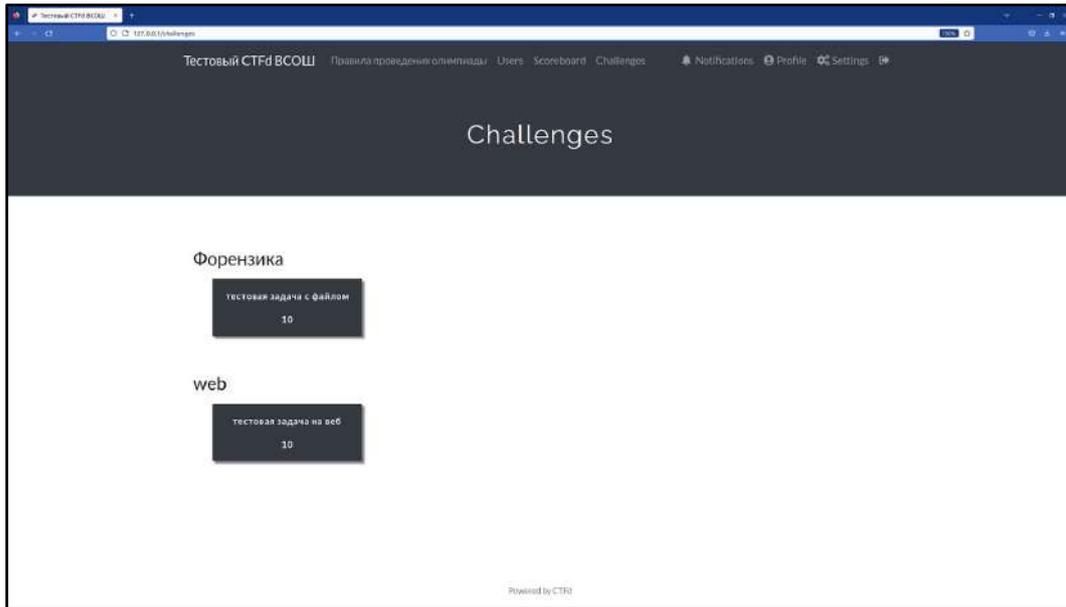


Рисунок 1 – примерный вид экранного интерфейса Платформы с заданиями

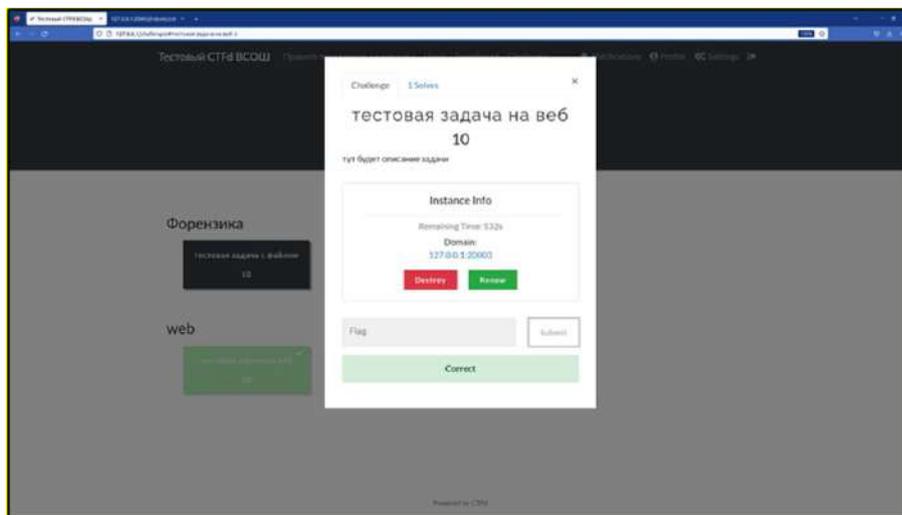
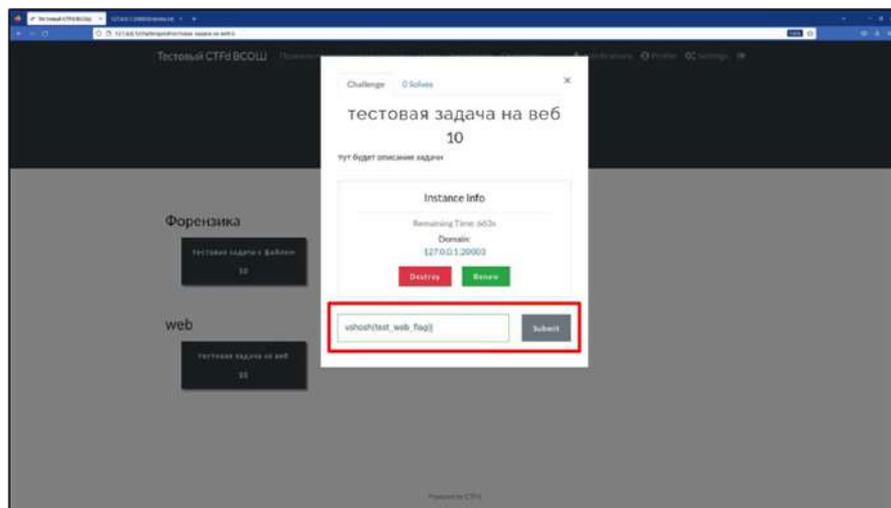


Рисунок 2 – пример успешного ввода флага. Задание засчитано.

Карта разбалловки для 11 классов

№ Задания	Тематика задания	Критерии оценки	Кол-во баллов
1.	СЗИ-1	Факт размещения участником в поле для ввода корректного флага	3
2.	Web 1	Факт размещения участником в поле для ввода корректного флага	5
3.	Forensics 1	Факт размещения участником в поле для ввода корректного флага	4
4.	Forensics 2	Факт размещения участником в поле для ввода корректного флага	4
5.	Reverse-1	Факт размещения участником в поле для ввода корректного флага	5
6.	Reverse-2	Факт размещения участником в поле для ввода корректного флага	5
7.	СЗИ-2	Критерии оценки приведены в задании	4
8.	СЗИ 3 + Анализ трафика	Критерии оценки приведены в задании	5
Σ			35

Задания

СЗИ 1 – Государственная тайна

Товарищ! Произошла авария на «Предприятии 3826», помоги расследовать все инциденты! Похоже в самом начале роботы зашифровали файл с секретными данными. К счастью, всё необходимое для расшифровки у нас есть – расшифруй данные роботов!

Рекомендуемые утилиты: openssl, bash.

Цель работы: получение доступа к флагу.

Итог работы: получить доступ до флага.

Критерий оценки: предоставление правильного флага.

Web 1 – КиберМаглев

На «Предприятии 3826» внедрили внутренний сервис для сотрудников, призванный улучшить коммуникацию и эффективность работы. Однако из-за сжатых сроков и отсутствия тестирования в системе осталась незамеченной ошибка, ставящая под угрозу конфиденциальность данных каждого инженера! Товарищ, помогите нам выявить проблему, а в качестве подтверждения предоставьте содержимое первого сообщения, отправленного инженером Петровым.

Рекомендуемые утилиты: BurpSuite, Python.

Цель работы: исследование логики работы web-приложения и получение доступа к флагу.

Итог работы: получить доступ до флага.

Критерий оценки: предоставление корректного флага.

Forensics 1 - Чертежи ТСП-23

В локальной сети комплекса засекли подозрительную активность. Кто-то пытается слить данные о новой модели Тяжелого Служебного Полимера внешним контрагентам. Найдите улики, подтверждающие факт утечки в перехваченном трафике.

Рекомендуемые утилиты: Wireshark, openssl, python.

Цель работы: исследование дампа памяти операционной системы и сетевого трафика

Итог работы: получить доступ до флага.

Критерий оценки: предоставление правильного флага.

Forensics 2 - Квантовый Провал

В секретной квантовой лаборатории товарища Петрова произошел критический сбой в экспериментальном вычислителе. В момент коллапса квантовой функции часть памяти оказалась фрагментирована по разным адресным пространствам. В руинах цифрового хаоса обнаружен скрипт квантовой автоматизации, который, похоже, пытается собрать воедино разрозненные кусочки секретного кода. Нужно восстановить данные до того, как квантовая декогеренция сделает их бесполезными.

Получившийся флаг из нескольких составных частей для сдачи в тестирующую систему оберните в префикс: vsosh{найденный_в_задании_флаг}. Итоговый формат флага: vsosh{0-9a-Z_!@}.

Рекомендуемые утилиты: volatility2, volatility3, dd.

Цель работы: исследование дампа памяти операционной системы.

Итог работы: получить доступ до флага.

Критерий оценки: предоставление правильного флага.

Reverse 1 - Коллектив 2.0

В лабораториях предприятия "3826" разработан новый протокол шифрования для доступа к экспериментальной версии нейросети "Коллектив 2.0". Этот протокол якобы способен остановить любую попытку взлома.

Ваша задача – изучить программу и алгоритм авторизации, обойти встроенную защиту и найти код доступа.

Рекомендуемые утилиты: IDA Free, Ghidra, GDB, python

Цель работы: определить алгоритм работы программы, восстановить секретное значение.

Итог работы: получить доступ до флага.

Критерий оценки: предоставление правильного флага.

Reverse 2 – Канарейка в серверной

На секретном объекте предприятия "3826" случился сбой, вызванный странным поведением робота-ученого. Легендарный инженер Петров разработал программу для защиты робота-ученого, но отвлекся на любимую робо-канарейку и случилась беда: система защиты оказалась уязвимой, и теперь не позволяет восстановить доступ к главному серверу.

Найдите и используйте слабость в защитной программе, чтобы вернуть контроль над системой.

Рекомендуемые утилиты: IDA Free, Ghidra, GDB, python (pwntools)

Цель работы: определить алгоритм работы программы, восстановить секретное значение

Критерий оценки: предоставление корректного флага

СЗИ 2 - База под угрозой

Товарищ! На нашем передовом объекте 'Предприятие 3826' зафиксирована подозрительная активность. Кажется, кто-то внес изменения в наш надежный код, обрабатывающий запросы к базе данных. Срочно необходимо заделать дыру в безопасности и предотвратить массовую утечку конфиденциальной информации о сотрудниках предприятия. Но учти, из-за массовых сетевых атак, онлайн-IDE работает с перебоями.

Рекомендуемые утилиты: python

Цель работы: изменение конфигурации приложения.

Итог работы: получить доступ до флага.

Критерий оценки: предоставление правильного флага.

СЗИ 3 - Сетевые движения

Товарищ! На 'Предприятии 3826' зафиксирована подозрительная активность в сетевой инфраструктуре. Робот отправляет опасные пакеты, вызывая сбои в системе управления. Наши детекторы уловили сетевые пакеты, но из-за остановки нейройИИ мы не можем их проанализировать. Твоя задача — разобрать сетевую активность в нашей сети, выявить все этапы возможной кибератаки и написать отчет “наверх” об атаке..

ВАЖНО: IP-адрес атакующего - индикатор решения задания, работы участников, некорректно \ не определивших его - не подлежат дальнейшей проверке! Решение разместите в сетевой папке, продублируйте на рабочем столе Вашей виртуальной машины участника.

Критерии оценки:

- Корректно определен IP-адрес атакующего - 1 балл
- Корректно определен флаг - 1 балла
- Корректно описана цепочка проведения атаки - 2 балла
- Корректно определен пароль пользователя mpalledorous - 1 балл

Рекомендуемые утилиты: Wireshark, hashcat

Цель работы: исследование вредоносной активности в записи трафика

Итог работы:

1. Сданный в тестовую систему IP-адрес атакующего
2. Текстовый файл report.txt с анализом хода атаки и заполненными полями (шаблон для заполнения приложен к заданию на платформе)