

**Практическое задание для заключительного этапа всероссийской олимпиады
школьников по технологии 2022 – 2023 учебный год
Профиль “Информационная Безопасность”, 10 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 кода (анализ исходных текстов компьютерных программ)
2. Web (поиск уязвимостей web-приложений)
3. Linux\Unix (навыки администрирования операционных систем)
4. Форензика (поиск следов инцидентов информационной безопасности)
5. 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).

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 в день проведения практического тура. Виртуальная машина с Платформой также должна быть доступна по локальной сети с машин участников.

5. 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).

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 выполняет 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>

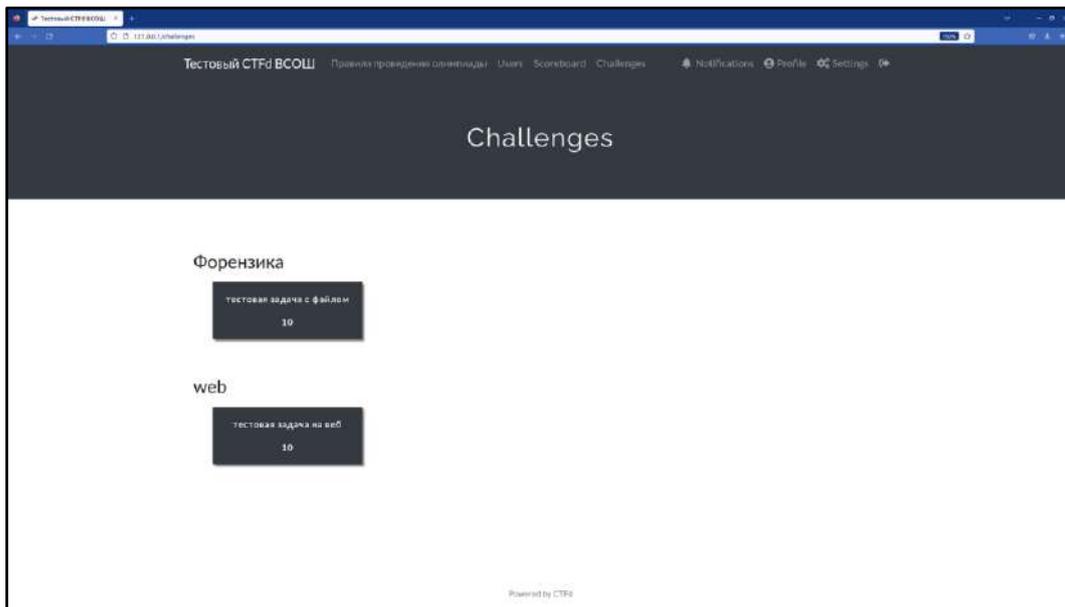


Рисунок 1 – примерный вид экранного интерфейса Платформы с заданиями

Порядок проведения

Длительность практического тура (выполнение практических заданий) для участников 9 класса составляет: 160 минут (без учета двух 10-ти минутных перерывов). В случае обнаружения неисправности в оборудовании, возникшей не по вине участника, по решению наблюдателя данный участник переседеть на ПК из числа зарезервированных на случай обнаружения неисправности в оборудовании, возникшей не по вине участника. Время, затраченное на выявление и устранение неисправности компенсируется.

Карта разбалловки для 10 классов

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

Задания

Реверс кода

В Реестр Российского ПО была внесена новая инновационная разработка инженеров из Сколково – блокнот! Они оставили демостенд для всех, чтобы люди смогли оценить гения инженерной мысли, однако кажется без уязвимостей не обошлось.

Подключение к сервису осуществляется через netcat: "nc <IP> <PORT>" IP адрес и порт появляются после поднятие инстанса задания.

Цель работы: исследование логики работы программы на языке C.

Итог работы:

- Требуется определить уязвимость в исходном коде;
- Проэксплуатировать эту уязвимость;
- При успешной эксплуатации уязвимости Вы получите доступ к флагу.

Критерий оценки: предоставление правильного флага.

Рекомендуемые предустановленные утилиты: gdb, ghidra, rizin, cutter, python3, pwntools, strace, ltrace, objdump, readelf.

Реверс кода

Петя впервые играет в CTF, но он неплохо разбирается в кодировках, возможно ему удастся получить флаг, вшитый в код в закодированном виде.

Цель работы: исследование логики алгоритма.

Итог работы: получить изначальную строку с флагом.

Критерий оценки: предоставление правильного флага.

Рекомендуемые предустановленные утилиты: python.

Web

После уязвимости с обходом двухфакторной аутентификации, выявленной школьниками 9ого класса, были предприняты меры по проектированию более безопасной логики работы механизмов аутентификации. Смогли ли программисты сделать неуязвимую двухфакторку?

Админ поделился своим логином и паролем admin:password, чтобы сфокусироваться лишь на двухфакторке (2FA).

Цель работы: исследование логики работы веб-приложения.

Итог работы: войти в аккаунт и получить доступ к флагу.

Критерий оценки: предоставление корректного флага.

Рекомендуемые предустановленные утилиты: BurpSuite, python requests.

Web

Один из сайтов, который изучал аналитик безопасности, выглядит *кхм* странно. Чтобы сдать корректный отчет и получить премию, нужно вытащить какую-нибудь чувствительную информацию.

Цель работы: исследование логики работы веб-приложения.

Итог работы: найти чувствительную информацию среди содержимого сервера.

Критерий оценки: предоставление корректного флага.

Рекомендуемые предустановленные утилиты: BurpSuite, python requests

Linux\Unix

Крутыми русскими хакерами была пробита внешка и получен доступ к серверу организации по ssh. Получится ли им получить полный доступ до root?

Первоначальное подключение к серверу происходит по логину паролю test:test (порт ssh сервера указан после поднятия задания)

Цель работы: исследование логики работы сервера.

Итог работы: считать содержимое файла /root/flag.txt

Критерий оценки: предоставление корректного флага.

Рекомендуемые предустановленные утилиты: bash

Анализ трафика

Исследовательскому отделу космической станции было поручено разобраться в крушении одного из спутников, однако все что осталось для проведения экспертизы – запись трафика.

Помогите команде провести расследование.

Ответ на это задание используется далее в задании “СЗИ”.

Для этого:

1. определите IP-адрес атакующего (**внесите найденный IP в поле флага**),
2. максимально подробно определите тип атаки (**описание предоставьте файле task7.txt на рабочем столе Вашей виртуальной машины участника и сетевой папке**),
3. опишите ход решения (**описание предоставьте файле task7.txt на рабочем столе Вашей виртуальной машины участника и сетевой папке**).

Цель работы: анализ трафика для выявления IP-адреса атакующего и типа атаки.

Итог работы:

1. Сданный (в качестве флага) в тестовую систему IP-адрес атакующего
2. Текстовый файл с корректно записанным типом атаки и ходом решения (обоснованием определения типа атаки)

Критерии оценки:

- Корректно определен IP-адрес атакующего - 1 балл
- Корректно определен вид атаки и описан ход решения - 1 балла

СЗИ

Продолжение задачи “Анализ трафика”: помогите предотвратить инциденты, подобные описанному, в будущем. Для найденного IP-адреса и типа атаки:

1. создайте правила межсетевого экрана iptables для предотвращения данной атаки,
2. по возможности выполните условия (ниже) на дополнительные баллы.

Внимание: если IP-адрес и тип атаки были определены в задании “Анализ трафика” неверно, данное задание также будет признано выполненным неверно!

Цель работы: создание цепочки правил iptables для блокировки атаки, представленной в исследуемой записи трафика (см. задание “Анализ трафика”).

Требования (3 балла):

1. В качестве названия цепочки правил – укажите предполагаемый вид атаки;
2. Укажите предельное число пакетов в единицу времени (пакеты будут проходить правило только после превышения ограничения) равным 1 в секунду;
3. Укажите максимальное значение счетчика пакетов, при котором срабатывает ограничение равным 2 пакетам.

Условие на дополнительные баллы: напишите shell-скрипт (.sh) для блокировки атаки (2 балла)

Итог работы:

1. Сданный (в качестве флага) в тестовую систему правильный IP-адрес атакующего
2. Текстовый файл с верно записанным типом атаки и ходом решения

Критерии оценки:

- Создано и работоспособно правило iptables для блокировки атаки - 3 балла
- За каждое отсутствующее требование - минус 1 балл
- Выполнено доп. условие (.sh скрипт подгружающий правила) - 2 балла