Практическое задание для заключительного этапа всероссийской олимпиады школьников по технологии 2022 – 2023 учебный год
Профиль “Информационная Безопасность”, 9 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. Форензика (поиск следов инцидентов информационной безопасности)
4. Linux\Unix (навыки администрирования операционных систем)
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 задний по тематики 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 VirtualBox[1].
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 ранее чем за 1 день до 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

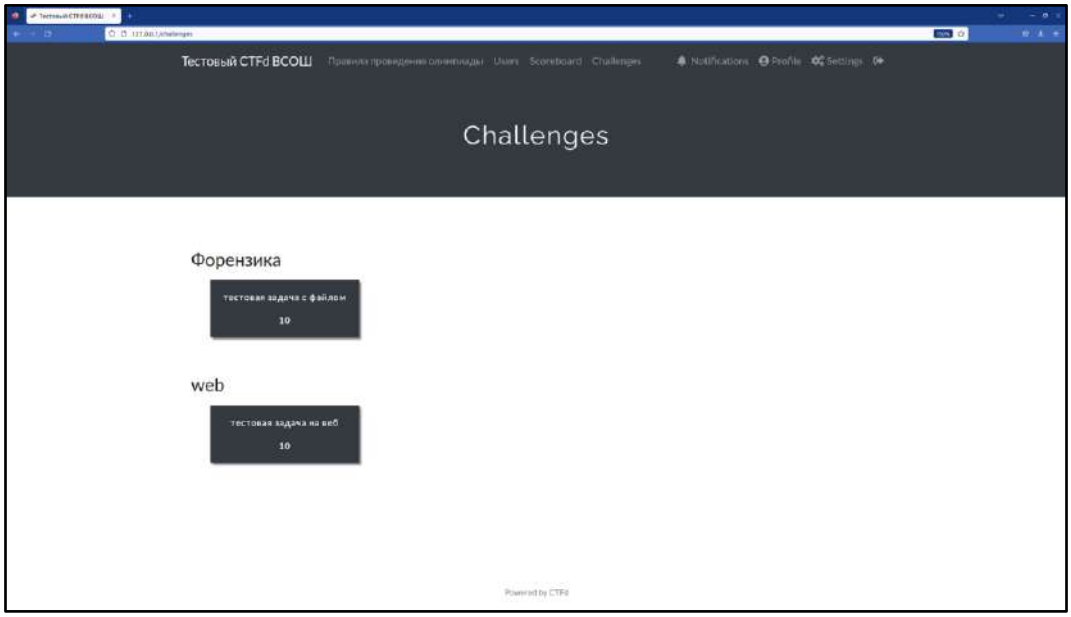

Рисунок 1 – примерный вид экранного интерфейса Платформы с заданиями

Порядок проведения

Длительность практического тура (выполнение практических заданий) для участников 9 класса составляет: ___ минут (без учета перерывов). В случае обнаружения неисправности в оборудовании, возникшей не по вине участника, по решению наблюдателя данный участник может пересесть на резервный ПК. Время, затраченное на выявление и устранение неисправности компенсируется.

Карта разбалловки для 9 классов

№ Задания	Тематика задания	Критерии оценки	Кол-во баллов
1.	Реверс кода	Факт размещения участником в поле для ввода корректного флага	8
2.	Web	Факт размещения участником в поле для ввода корректного флага	4
3.	Web 2	Факт размещения участником в поле для ввода корректного флага	8
4.	Форензика	Факт размещения участником в поле для ввода корректного флага	4
5.	Форензика	Факт размещения участником в поле для ввода корректного флага	4
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 эксплуатация уязвимости Вы получите доступ к флагу.

Критерий оценки: предоставление правильного флага.

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

Web

Админ серверной в трёхбуквенной организации потерял доступ к своему мобильному телефону и не может пройти двухфакторную аутентификацию, однако ему крайне необходимо получить доступ к своему аккаунту несмотря на столь обидную утрату! Возможно стоит положиться на халатность программистов, которые проектировали личный кабинет сотрудника.

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

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 2

Лучшие фронтенд-инженеры России проектировали сайт где крайне счастливый хранитель флага хочет показать его вам! Однако бекенд-разработчики решили устроить сюрприз и забанили всех по айпи!! Конкуренция двух лагерей пока не привела к успешному получению флага, однако, возможно, победа крайне близко...

Цель работы: исследование логики работы веб-приложения.

Итог работы: обойти блокировку по ip адресу и получить доступ до флага.

Критерий оценки: предоставление корректного флага.

Рекомендуемые предустановленные утилиты: BurpSuite

Форензика

Обычный школьник Иван из Твери нашёл флешку бывшего крипто-шейха с приватным ключом от его кошелька. Однако криптошейх не так прост и попытался максимально усложнить получение ключа. Вероятно, он недооценил уровень Российского образования.

Цель работы: получение доступа к флагу.

Итог работы: получить доступ до флага.

Критерий оценки: предоставление корректного флага.

Рекомендуемые предустановленные утилиты: bash, python

Форензика

Борис собирал пожертвования на криптокошелёк на школу юных хакеров в Сирии, за что был похищен агентами ФБР. Пока черный самолет с Борисом летит в Гуантанамо, у вас совсем немного времени, чтобы узнать пароль от кошелька и спасти собранные средства. Наверняка он хранил его где-то на сервере — доступ по ssh, аккаунт Boris:pass-for-ssh. Последнее сообщение от Бориса было очень странным: 226 315 28 9 449 997 113 4500 7777

Первоначальное подключение к серверу происходит по логину паролю Boris:pass-for-ssh (порт ssh сервера указан после поднятия задания);

Цель работы: получение доступа к флагу.

Итог работы: получить корректный флаг из содержимого файлов, расположенных на сервере.

Критерий оценки: предоставление корректного флага.

Рекомендуемые предустановленные утилиты: bash, python

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 3 пакета в секунду;
3. Укажите максимальное значение счетчика пакетов, при котором срабатывает ограничение равным 3 пакетам.

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

Итог работы:

1. Текстовый файл с написанной цепочкой правил
2. shell-скрипт подгружающий правила

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