Практическое задание заключительного этапа
всероссийской олимпиады школьников по технологии 2023 – 2024 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. Reverse (анализ исходных текстов программ)
2. Reverse (PWN) (эксплуатация бинарных уязвимостей программ)
3. Web (поиск уязвимостей web-приложений)
4. Linux\Unix (Misc) (задания смешанной категории, навыки работы в ОС Linux\Unix)
5. СЗИ (Средства защиты информации).

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

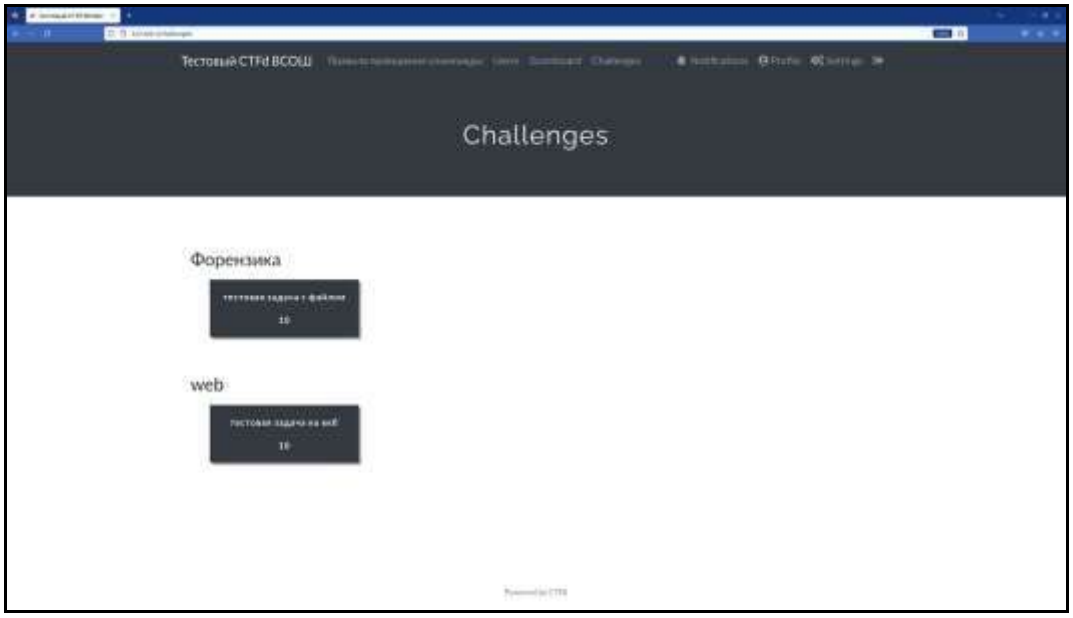

Рисунок 1 – примерный вид экранного интерфейса Платформы с заданиями

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 11 классов

№ Задания	Тематика задания	Критерии оценки	Кол-во баллов
1.	**Linux\Unix (Misc)**	Факт размещения участником в поле для ввода корректного флага	3
2.	**Web**	Факт размещения участником в поле для ввода корректного флага	4
3.	**Web**	Факт размещения участником в поле для ввода корректного флага	8
4.	**Reverse**	Факт размещения участником в поле для ввода корректного флага	7
5.	**Reverse (PWN)**	Факт размещения участником в поле для ввода корректного флага	7
9.	**СЗИ**	Критерии оценки приведены в задании	6
			35

Задания

Misc - Хастад

Сквозь дымку болот и гущу интриг явился я - Хаст, ваш верный слуга. Уже пробрались мы в самое сердце тёмной сети этих коварных злодеев. После многодневного наблюдения стало понятно, что вождь этой гнилой шайки периодически распределяет одинаковые секретные ключи множеству своих последователей. До недавнего времени нашим мастерам удавалось разгадывать каждое послание, однако недавно какой-то хитрец внедрил непонятную систему защиты. Наши ушки, пока что, не заметили этой переменчивой уловки. Возможно, вам, благородный путник, удастся помочь нам в этом древнем противостоянии?

Рекомендуемые используемые утилиты: WireShark, python

Цель работы: получение доступа к флагу

Итог работы: получить доступ до флага

Критерий оценки: предоставление правильного флага

Web - Секретная система

[ДАННЫЕ УДАЛЕНЫ] [ДАННЫЕ ЗАСЕКРЕЧЕНЫ]. Найдите возможность получить данные в новой зелёно-чёрной системе Дийкстры.

Рекомендуемые используемые утилиты: BurpSuite, [ДАННЫЕ УДАЛЕНЫ]

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

Итог работы: получить доступ до флага

Критерий оценки: предоставление корректного флага

Web - Синдром низушка

Простой низушек является лишь гостем (guest) в этих землях, однако пытается выдать себя за администратора земель. С собой он прихватил секретные и публичные файлы, как жаль что администратор использует другие!

Рекомендуемые используемые утилиты: BurpSuite, jwt editor, jwt_tool, python, openssl

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

Итог работы: получить доступ до флага

Критерий оценки: предоставление корректного флага

Reverse - Do You Know The Way?

В темных краях программного кода, в часы, когда мрак окутывает каждую строку, заклинание властвует над самим собой - само себя изменяет, тайно переписывая свои заклинания, и скрывает проверки флагов, словно туманный пеленой, окутывающей истину. Задание состоит в том, чтобы разгадать этот коварный обман, раскрыть тайны программного кода и пройти скрытые испытания, как настоящий охотник на чудовищ.

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

Цель работы: исследование логики работы программы

Итог работы: определить уязвимость в исходном коде, поэксплуатировать эту уязвимость, получить доступ к флагу

Критерий оценки: предоставление корректного флага

PWN - Return

В библиотеке Аретузы Вы нашли волшебного кота, но он ничего не делает - только спит. Попробуйте, обойти его, найти нужный адрес и получить доступ к книге "secret.txt", открыв три замка и не разбудив кота хранителя

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

Прим.: флаг находится в файле "secret.txt"
Рекомендуемые используемые утилиты: Python, pwntools

Цель работы: исследование логики работы программы

Итог работы: определить логику работы программы, получить доступ к флагу

Критерий оценки: предоставление корректного флага

СЗИ - Тайны Сети

Сетевой маг Элиан утверждает, что помогал другу с тестированием сайта, но тьма подозрений окутывает его слова. Ведьмаки, стражи магии и реальности, зовутся раскрыть эту тайну. Помоги нам разгадать шифры сети и разоблачить загадочную активность, что таится внутри вихря данных.

ВАЖНО: Вредоносный файл создан на основе реального образца, не запускать на хостовой машине. 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 определены контакты, название группировки, C&C - 1 балл
• Проведен и расписан анализ кода вредоносного файла - 2 балла
• Создано правило iptables для блокировки аналогичных обращений - 1 балл
• Выполнено доп. условие (.sh скрипт подгружающий правила) - 1 балл

Рекомендуемые используемые утилиты: Wireshark, iptables, pycdc, pyinstxtractor-ng

Цель работы: исследование вредоносной активности в записи трафика

Итог работы:
1. Сданный в тестовую систему IP-адрес атакующего
3. Текстовый файл report.txt с анализом кода вредоносного файла и заполненными полями (шаблон для заполнения приложен к заданию на платформе)
2. Текстовый файл с написанной цепочкой правил
3. shell-скрипт подгружающий правила