Практическое задание для регионального 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. Реверс (анализ исходных текстов компьютерных программ)
2. Web (поиск уязвимостей web-приложений)
3. Forensics (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 заданий по тематике СЗИ производится организаторами на основании предоставленных участниками файлов.

Максимально возможное число баллов за практический тур – 35 баллов.

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.

[1] https://www.virtualbox.org/wiki/Downloads

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 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.

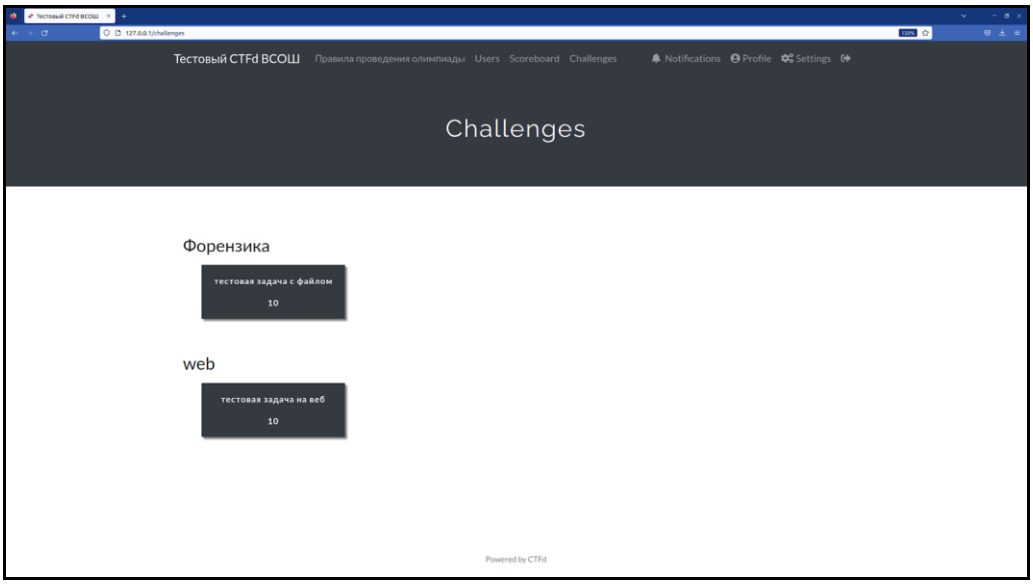

Рисунок 1 – примерный вид экранного интерфейса Платформы с заданиями

Порядок проведения

Длительность практического тура (выполнение практических заданий) для участников 11 класса составляет: 180 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 такой неисправности, компенсируется.

Шифр участника _____

Карта оценки участника регионального этапа – 11 класс

№ задания	Тематика задания	Критерии оценки	Всего баллов	Баллы по факту
1.	**Linux\Unix (misc)**	Факт размещения участником в поле для ввода корректного флага	**1**	
2.	**Linux\Unix (adm)**	Факт размещения участником в поле для ввода корректного флага	**2**	
3.	**Forensics**	Факт размещения участником в поле для ввода корректного флага	**3**	
4.	**Web**	Факт размещения участником в поле для ввода корректного флага	**3**	
5.	**Web**	Факт размещения участником в поле для ввода корректного флага	**5**	
6.	**Reverse**	Факт размещения участником в поле для ввода корректного флага	**3**	
7.	**Reverse**	Факт размещения участником в поле для ввода корректного флага	**5**	
8.	**Reverse (pwn)**	Факт размещения участником в поле для ввода корректного флага	**6**	
9.	**СЗИ**	Критерии оценки приведены в задании	**2**	
10.	**СЗИ + Анализ трафика**	Критерии оценки приведены в задании	**5**	
Σ			**35**	

Задания

Linux\Unix (misc) - флешка возможностей
Обыкновенный тинейджер Лютик наткнулся на безобидно выглядывающую из одуванчиков флешку. "БЕСПЛАТНО" - подумал Лютик, но оказалось, что это не просто флешка, а целый булыжник цифровых тайн, оставленный на память неким загадочным чародеем, который решил замутить такую загадочную игру на выуживание ключа доступа, что сам бы в ней не справился… тут не обойтись без чеканной монеты.

Цель работы: получение доступа к флагу

Итог работы: получить доступ до флага

Критерий оценки: предоставление правильного флага

Рекомендуемые предустановленные утилиты: bash, python

Linux\Unix (adm) - pam postexploiatation
На одном из веб серверов Крепости Старого Моря заметили подозрительную активность – теперь там обитают чудовища... кто-то может входить в любые аккаунты - что же произошло? Для решения задания найдите флаг в скомпроментированной системе

Цель работы: исследование дампа системы

Итог работы: найти флаг в скомпрометированной системе

Критерий оценки: предоставление корректного флага

Рекомендуемые предустановленные утилиты: bash, python

Forensics - ransome lab incident
Очередной заказ... у нашего клиента – купца лишь дубликат зачарованной системы ... все свитки затемнены магическим шифром... ПОМОГИТЕ мне расшифровать таинственный пергамент с рунами на на рабочем столе.

Цель работы: исследование дампа системы

Итог работы: получить доступ до флага (определить логику шифровальщика и дешифровать файл)

Критерий оценки: предоставление корректного флага.

Рекомендуемые предустановленные утилиты: bash, python

Сокеты в вебе
Вы обучаетесь Аретузе, фанат транспорта и не любите приложения? Придумали классный костыль - лучшее из обоих миров!

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

Итог работы: получить доступ до флага

Критерий оценки: предоставление корректного флага

Рекомендуемые предустановленные утилиты: Burp Suite, python

Web - по ошибкам вслепую
После того, как Геральт из Ривии успешно победил монстра, появилось новое испытание – взломать систему древних магов, построенную на структурированном хранилище данных, где по некоторым предположениям, хранится важная информация о Предназначении.
Ваша миссия заключается в том, чтобы проэксплуатировать потенциальные уязвимости в обходе ограничений ввода данных, которые могут позволить изменять структуру запросов к этому хранилищу. Помните, что ведьмаку полезно не только знать, как взаимодействовать с живыми существами, но и как взломать системы без использования традиционной sql-инъекции.

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

Итог работы: получить доступ до флага

Критерий оценки: предоставление корректного флага

Рекомендуемые предустановленные утилиты: Burp Suite, python

Reverse - heap
Даже силами студентов академии Артуза не остановить этот импортозамещающий вихрь магии - перед нами очередной тестовый стенд, залитый сиянием аргументов. Проверим же, насколько безопасно все в этот раз…

Ведьмак Геральт, его ученица Цири и спутница Йеннифер внимательно изучают магическую конструкцию. Хаотично мерцающие руны на каменной башне среди не предвещают ничего хорошего. Но нашим героям не впервой сталкиваться с неизвестностью и опасностью.

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

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

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

Reverse - crackme

Школьница-ведьма из Новиграда, Маргарита, обнаружила в "Виноградном Сообществе" свиток с программой-заклинанием на захват власти. Бывший владелец свитка исчез, поэтому ей придется разобраться в древней программной магии самостоятельно. К счастью, школа в Лодии уже давно обучает таким навыкам.

Цель работы: исследование логики работы программы

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

Критерий оценки: предоставление корректного флага

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

Reverse (pwn) - free me up

Тайный код для активации Ведьмачьего знака Игни - НОЛЬ НОЛЬ НОЛЬ НОЛЬ НОЛЬ НОЛЬ НОЛЬ НОЛЬ. Предложенный код действовал с 1060 по 1127 год, в эпоху Великого Ведьмака. Однако Геральт и Цири родились еще позже, в 1290 году, и этот код, к сожалению, для них не подходит. Помогите нашим Белому Волку и Ласточке раскрыть секретную последовательность и активировать знак Игни, чтобы спасти мир, изувеченный войной с Нильфгаардом.

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

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

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

СЗИ - just nginx

Геральт из Ривии получает новое задание. Сетевой демон NGINX уязвим для Сил Зла, нужно его проанализировать и исправить уязвимости в конфиге. Этот заказ потребует от Ведьмака знаний в кодинге…помогите Геральту выполнить миссию.

Цель работы: определение и исправление уязвимости в конфигурации nginx

Итог работы:
загрузите в предоставленные формы 2 файла:
1. текстовый файл с описанием уязвимости
2. исправленный конфигурационный файл

Критерии оценки:
• Корректно определена уязвимость - 1 балл
• Корректно исправлен конфигурационный файл - 2 балла
• НЕ корректно определена уязвимость - минус 1 балл
• Отсутствует описание уязвимости - минус 0.5 балла

Анализ трафика

На Скеллиге произошло что-то страшное, однако все что осталось Йеннифэр и Мышовуру для проведения экспертизы - запись трафика. Помогите чародейке и друиду провести расследование дабы предотвратить подобные инциденты в будущем. Для этого: определите IP-адрес атакующего, определите тип атаки, создайте правила iptables для предотвращения данной атаки.

Решение разместите в сетевой папке, продублируйте на рабочем столе Вашей виртуальной машины участника.

ВАЖНО: IP-адрес атакующего - индикатор решения задания, работы участников, некорректно \ не определивших его - не подлежат дальнейшей проверке!

Целью работы является цепочки правил iptables для блокировки атаки, представленной в исследуемой записи трафика.

При этом требования к правилу iptables:
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 1

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

Итог работы:

1. Сданный в тестовую систему IP-адрес атакующего
2. Текстовый файл с написанной цепочкой правил
3. shell-скрипт подгружающий правила

Критерии оценки:

• Корректно определен IP-адрес атакующего - 1 балл
• Корректно определен вид атаки - 1 балла
• Создано правило iptables для блокировки атаки - 2 балла
• За каждое отсутствующее требование - минус 1 балл
• Выполнено доп. условие (.sh скрипт подгружающий правила) - 2 балла