Практическое задание для заключительного этапа всероссийской олимпиады школьников по труду (технологии) 2024 – 2025 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 (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 некоторых заданий 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 отдельных заданий СЗИ производится организаторами на основании предоставленных участниками файлов.

Максимально возможное число баллов за практический тур – 35 баллов.

Время на изучение инструкции не входит в общее время выполнения заданий.

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

Инфраструктура и инструкция 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 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 CTFd 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 10 класса составляет: **не менее 3 часа 30 мину**т (без учета перерывов).

Общие требования

1. До начала практического тура необходимо обеспечить доступ с ПК участников к Платформе с заданиями, развернутой на сервере.

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 некоторых заданий СЗИ) вводятся на Платформе. Количество попыток ввода флага не ограничено. За ошибочно введенный флаг баллы не снижаются. Успешно найденный флаг содержит следующий формат - vsosh{*найденный_флаг*}, в любом регистре.

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

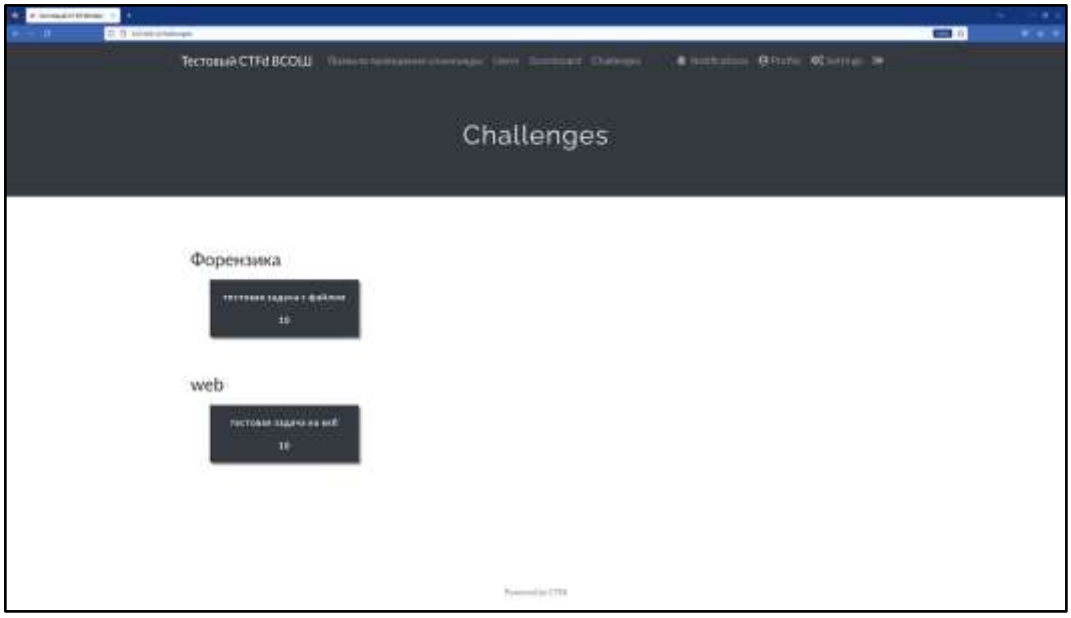

Рисунок 1 – Примерный вид экранного интерфейса Платформы с заданиями

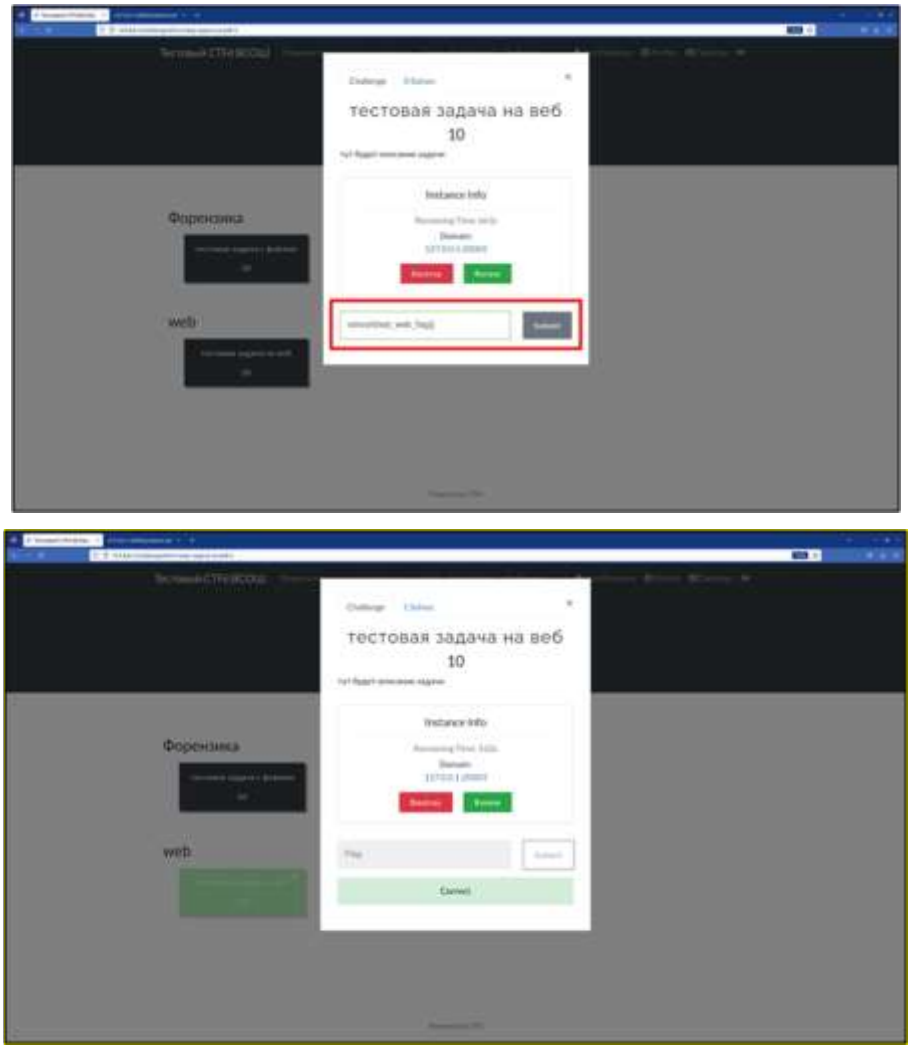

Рисунок 2 – Пример успешного ввода флага. Задание засчитано.

Карта разбалловки для 10 классов

№ Задания	Тематика задания	Критерии оценки	Кол-во баллов
1.	**СЗИ 1 “Энклейв”**	Факт размещения участником в поле для ввода корректного флага	**1**
2.	**Web 1 “КиберКонвейер”**	Факт размещения участником в поле для ввода корректного флага	**5**
3.	**Web 2 “Гонки за оборудованием”**	Факт размещения участником в поле для ввода корректного флага	**2**
4.	**Forensics 1 “Порча модуля памяти Коллектора”**	Факт размещения участником в поле для ввода корректного флага	**1**
5.	**Forensics 2 “Зашифрованные коммуникации”**	Факт размещения участником в поле для ввода корректного флага	**3**
6.	**Forensics 3 “Квантовый хаос”**	Факт размещения участником в поле для ввода корректного флага	**4**
7.	**Reverse 1 “Полимерный замок”**	Факт размещения участником в поле для ввода корректного флага	**5**
8.	**Reverse 2 “Matreshka”**	Факт размещения участником в поле для ввода корректного флага	**2**
9.	**PWN “Операция Эхо”**	Факт размещения участником в поле для ввода корректного флага	**5**
10.	**СЗИ 2 “Сетевой дозор”**	Факт размещения участником в поле для ввода корректного флага	**1**
11.	**СЗИ 3 “База снова под угрозой”**	Факт размещения участником в поле для ввода корректного флага	**3**
12.	**СЗИ 4 + Анализ трафика “Сетевые движения”**	Критерии оценки приведены в задании	**3**
Σ			**35**

Задания

СЗИ 1 – Энклейв

Товарищ офицер! Наши союзники, генномодифицированные орлы, нашли рядом с секретным убежищем в горах Калифорнии флешку со странным гербом и зашифрованными файлами. Видимо, кто-то уронил при посещении объекта. Разведка считает, что на ней могут быть данные о секретной организации “Анклав” – тайной военно-политической организации США. Просим оказать помощь в расшифровке файла и поиске в нем секретной информации.

Рекомендуемые утилиты: openssl, bash.

Цель работы: получение доступа к флагу.

Критерий оценки: предоставление правильного флага.

Web 1 – КиберКонвейер

На “Предприятии 3826” установили платформу, документирующую сложные процессы сборки и тестирования роботизированных узлов. Недавно выяснилось, что в её механизмах присутствует уязвимость, способная влиять на критически важные данные. Необходимо понять, как она появилась, и устранить опасность прежде, чем сбои затронут всё производство!

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.

Web 2 – Гонки за оборудованием

Внутри «Предприятия 3826» уже долгое время исправно работает система выдачи оборудования по карточкам. Однако недавно было обнаружено, что один из инженеров смог взять больше оборудования, чем позволяется, тем самым нарушим работу распределительной системы. Помогите нам локализовать изъян, определив его первопричину!

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 – Порча модуля памяти Коллектора

Во время планового обновления прошивки модели "Коллектор-12Б" произошел критический сбой. Робот-уборщик высшего класса, задействованный в сборе образцов на территории "Предприятия 3826", вошел в экстренный режим отладки и сбросил аварийный дамп. Технический отдел установил, что в памяти устройства могли остаться ключевые данные о местоположении экспериментальных образцов Нейрополимера, доступ к которым требует восстановления удаленных фрагментов из поврежденной файловой системы.

Рекомендуемые утилиты: foremost, photorec, testdisk, binwalk.

Цель работы: исследование файла с данными.

Критерий оценки: предоставление правильного флага.

Forensics 2 – Зашифрованные коммуникации

В ходе секретной операции по слежению за подозрительной активностью в сети, вы перехватили HTTPS-трафик между неизвестным агентом и сервером. Вместе с трафиком был обнаружен файл с ключами сессии, что даёт возможность расшифровать данные и выяснить, какие действия предпринимает агент.

Рекомендуемые утилиты: Wireshark, tshark, python.

Цель работы: исследование дампа сетевого трафика.

Критерий оценки: предоставление правильного флага.

Forensics 3 – Квантовый хаос

После сбоя в экспериментальном квантовом процессоре часть памяти исследовательской станции оказалась фрагментирована. В памяти находится скрипт, который может собрать части флага, разбросанные по разным областям памяти.

Рекомендуемые утилиты: volatility2, volatility3.

Цель работы: исследование дампа памяти ОС.

Критерий оценки: предоставление правильного флага.

Reverse 1 – Полимерный замок

В лабораториях "Предприятия 3826" был обнаружен засекреченный модуль управления "Полимерным Замком". Этот модуль отвечает за контроль доступа к критически важным объектам. Но после инцидента с Полимером все системы перешли в аварийный режим, блокируя даже легитимных пользователей. Верните контроль над системой!

Рекомендуемые утилиты: IDA Free, Ghidra, GDB, python

Цель работы: определить алгоритм работы программы, восстановить секретное значение

Критерий оценки: получение корректного флага

Reverse 2 – Matreshka

В недрах Комплекса хранятся тайны, скрытые от посторонних глаз. Директива Р-16/7 засекречена высшим руководством, но фрагмент данных просочился через систему. Его рабочая станция обнаружена с единственным активным файлом. Твоя задача, товарищ, исследовать полученную информацию. Комплекс рассчитывает на твои аналитические способности.

Рекомендуемые утилиты: python

Цель работы: восстановить секретное значение

Критерий оценки: получение корректного флага

PWN 1 – Сломанный Механизм

Товарищ! Наши инженеры разработали экспериментальную систему управления, но в процессе тестирования обнаружились аномалии в работе одного из критических модулей. Программа ведет себя нестабильно при обработке определенных входных данных, а в её логике явно прослеживаются следы опасной уязвимости.

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

Цель работы: поиск и эксплуатация уязвимости в бинарном приложении

Критерий оценки: получение корректного флага

СЗИ 2 – Сетевой дозор

Товарищ, нам срочно нужен доступ до консоли управления Предприятием. Однако атакованные роботы все обложили своими слоями защиты. Найди в них лазейку и узнай с каким адресом и протоколом прикладного уровня можно пройти сквозь эту защиту 3-го уровня.

Формат флага: vsosh{ip_protocol}. Пример: vsosh{192.168.1.0_http}

Рекомендуемые утилиты: iptables

Цель работы: получение корректного флага

Критерий оценки: флаг в формате: предоставление правильного флага

СЗИ 3 – База снова под угрозой

Товарищ, нам снова требуется твоя помощь! На передовом объекте 'Предприятие 3826' вновь зафиксирована подозрительная активность. Нарушители добрались до нашего кода и внесли изменения в механизм обработки и выполнения запросов к БД. Твоя задача – как можно скорее устранить дыру в безопасности и не позволить злоумышленникам получить наши секретные данные. Обращаем внимание, что из-за большой нагрузки наша онлайн среда разработки работает с перебоями, наберись терпения. Удачи!

Рекомендуемые утилиты: python.

Цель работы: изменение конфигурации приложения.

Итог работы: получить доступ до флага.

Критерий оценки: предоставление правильного флага.

СЗИ 4 – Сетевые движения

Сетевая инфраструктура “Предприятия 3826” все еще под угрозой - кажется кто-то ведет бурную разведку, даже нейроИИ прилег. Твоя помощь вновь нужна - необходимо разгадать последовательность действий атакующих и собрать сетевые артефакты. Не забудь вновь сделать отчет “наверх” и вписать адрес атакующего в систему, без этого никак.

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.

Рекомендуемые утилиты: Wireshark

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).

Критерии оценки:

- Корректно определен IP-адрес атакующего - 1 балл
- Корректно найден флаг, формата vsosh{} - 1 балл
- Корректно описана цепочка проведения атаки - 1 балл