Практическое задание для регионального этапа всероссийской олимпиады школьников по технологии 2022 – 2023 учебный год
Профиль “Информационная Безопасность”, 10-11 класс

Тематики заданий

В туре необходимо решить как можно больше заданий. Наборы заданий ориентированы на комплексную оценку навыков участников регионального тура и охватывают перечисленные ниже темы:

1. Web (поиск уязвимостей web-приложений);
2. Реверс кода (анализ исходных текстов компьютерных программ);
3. Анализ трафика (поиск следов инцидентов в сетевом трафике);
4. Linux\Unix (навыки администрирования операционных систем);
5. Форензика (поиск следов инцидентов информационной безопасности);
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 прислан перед началом тура), доступ к которому является индикатором успешного решения задания.

Оценка задний по тематики СЗИ производится организаторами на основании предоставленных участниками файлов/скриншотов.

Максимально возможное число баллов за практический тур – 35 баллов.

Инструкции для организаторов и участника приложены к данному документу (Приложение А и Б).

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 экзамена.
4. На сервере организаторов запускается виртуальная машина с Платформой с заданиями. Она используется для решения всех заданий, кроме заданий по работе с СЗИ. Инструкция по

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

развертыванию Платформы предоставлена в составе данного комплекта документов. 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. Например, через LMS, яндекс-формы, общие папки на сервере (индивидуальные папки с персональным доступом для каждого участника).

Виртуальные машины доступны для скачивания в сети Интернет во время проведения Олимпиады по ссылкам ниже:

Основная ссылка: https://miem.hse.ru/rosh/2023/download/vmlink_z

Резервная ссылка: https://drive.google.com/drive/folders/12PIhdH4fE4MhoG1h8fjsUG5MIn_9h43U

Логин / пароль платформы CTFd: admin / =qyXg~`%$VL7bz(y0^@tVpDmuJZ!Y0[)

Пароль ОС Ubuntu: qaK!Goa=10d

Пароль от zip-архива: l}NHH#Pl36&$*F$Q:ZYS_s&?pY:t)Og+

Общие требования

1. До начала практического тура необ
ходимо 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.

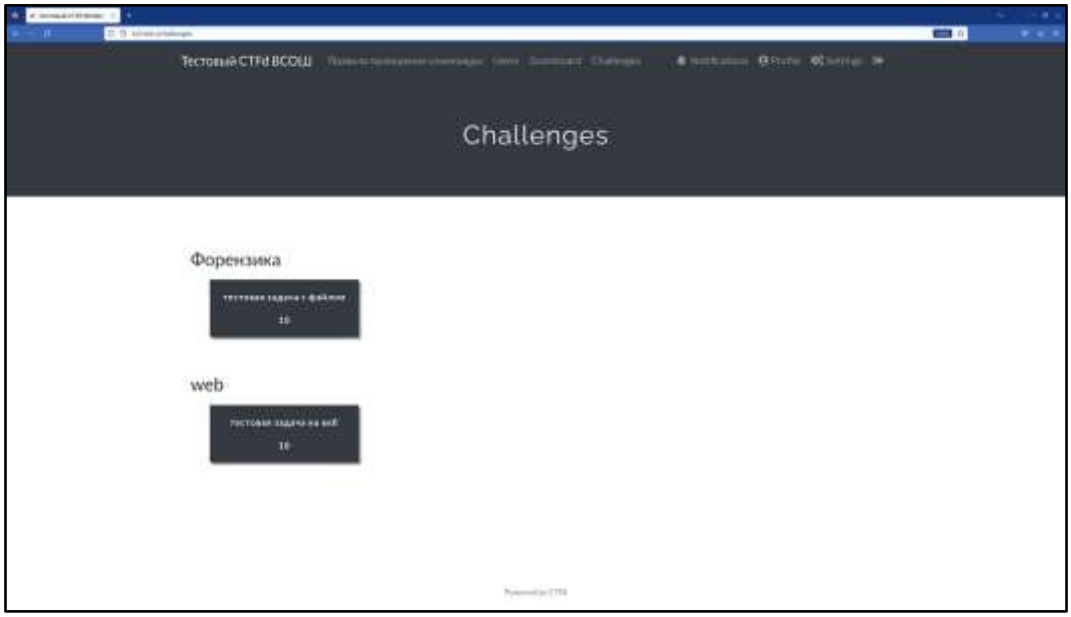

Рисунок 1 – примерный вид экранного интерфейса Платформы с заданиями

Порядок проведения

Длительность практического тура (выполнение практических заданий) для участников 10-11 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 пересесть 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 10-11 классов

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

Задания

Анализ трафика

На Web-сервере орбитальной станции был зафиксирован подозрительный трафик, после чего управление ею было перехвачено злоумышленниками. Вскоре экипаж получил анонимное сообщение "Я слышал, космонавты очень умные. Докажите это. Я верну вам управление станцией, если сможете найти в фрагментах трафика (.pcapng) и расшифровать мой ключик. Иначе вы все сгорите в атмосфере! Ахахаха!". Помогите экипажу расследовать данный инцидент и вернуть управление станцией.

Цель работы: является исследование записи трафика (.pcapng).

Итог работы: нахождение и декодирование флага, доступ к которому является индикатором успешного решения задания.

Критерий оценки: предоставление правильного флага.

Рекомендуемые предустановленные утилиты: WireShark, python3

Форензика

В отдел исследования инцидентов орбитальной станции прислали дамп файловой системы сервера. Вот бы найти флаг.

Целью работы является исследование дампа файловой системы сервера.

Итог работы: нахождение флага, доступ к которому является индикатором успешного решения задания.

Критерий оценки: предоставление корректного флага.

Рекомендуемые предустановленные утилиты: ftk imager/mount

Реверс кода

В отдел безопасности ПО орбитальной станции была прислана программа на языке
C. Подключение с помощью консольной утилиты netcat - "nc [host] [port]"

Целью работы является исследование логики работы программы на языке C. При этом:
• Требуется определить уязвимость в исходном коде;
• Проэксплуатировать этот уязвимость;
• При успешной эксплуатация уязвимости Вы получите доступ к флагу.

Итог работы**:** получение флага, доступ к которому является индикатором успешного решения задания.

Критерий оценки: предоставление корректного флага.

Рекомендуемые предустановленные утилиты: gdb, gcc и др.

Web

«Недавно узнал про xml, пока лишь разбираюсь, не судите строго» — сказал наш стажер отдела космических бэкендеров. Он явно плохо учился в школе и в разработанном им веб-сервисе есть уязвимости.

Целью является исследование логики работы веб-приложения. При этом:
• Требуется определить уязвимость в реализации веб-приложения;
• Требуется считать flag.txt из директории приложения, поэксплуатировав эту уязвимость.

Итог работы: нахождение флага, доступ к которому является индикатором успешного решения задания.

Критерий оценки: предоставление корректного флага.

Рекомендуемые предустановленные утилиты: Burp Suite

Web-2

Старый добрый PHP используется даже за пределами атмосферы Земли. Несмотря на небольшую уязвимость, которую я нашёл, полный удалённый доступ вряд ли возможен...

Целью работы является исследование логики работы веб-приложения. При этом:
• Требуется определить уязвимость в реализации веб-приложения;
• Необходимо считать файл со случайным названием из директории приложения, проэксплуатировав эту уязвимость.

Итог работы: нахождение флага, доступ к которому является индикатором успешного решения задания.

Критерий оценки: предоставление корректного флага.

Linux\Unix

Все бинарные файлы кодов запуска ракет должны быть в порядке. У нас же серьезный технический контроль и военная приёмка… Но на всякий случай, надо проверить.

Целью работы является исследование логики работы сервера. При этом:
• Первоначальное подключение к серверу происходит по логину паролю petya:pass-for-ssh (порт ssh сервера указан после поднятия задания);
• Необходимо считать содержимое файла с флагом, который находится в файловой системе.

Итог работы: нахождение флага, доступ к которому является индикатором успешного решения задания.

Критерий оценки: предоставление корректного флага.

Рекомендуемые предустановленные утилиты: hashcat, john

СЗИ №1

Создание дерева цифровых сертификатов.

Для корректной работы веб-сервиса управления космической станции, необходимо развернуть инфраструктуру открытых ключей (PKI). Для этого реализуйте скрипт с использованием OpenSSL по созданию цепочки цифровых сертификатов. Сгенерированные сертификаты (и вся цепочка доверия) не должны иметь ошибок, критических полей (кроме указанных) или неверных данных.

Целью работы является создание скрипта (.bat), который при запуске полностью автоматически создает дерево сертификатов из 3-х уровней. При этом:

• Корневой сертификат УЦ (root ca) – для “Space Station” ИЛИ «Космическая станция»

• Промежуточный ЦС (mca) - для Вашего класса (например, “Класс 11а”)

• Конечный (пользовательский, user) для себя (Name Surname)

При отображении в хранилище Windows дерево сертификатов должно отображаться без ошибок.

Закрытый ключ должен быть зашифрован.

Обязательно использование расширений:
• Ограничения цепочки - basicConstraints: для УЦ - без ограничений, ЦС - разрешить выдавать только пользовательские, Конечный - не ЦС)

Итог работы: загрузите в предоставленные формы 10 файлов:

• итоговые сертификаты (3 файла в формате .crt),

• скрипт для создания сертификатов (1 файл .bat)

• 1 конфигурационный файл openssl для создания сертификатов

• скриншоты: созданного дерева при просмотре в ОС Windows (1 файл) и вкладки Details каждого сертификата (3 файла) в цепочке просмотре в ОС Windows (чтобы были видны все расширения)

• файл PKCS

Использование русского языка в полях сертификата Субъект (Subject), Издатель (Issuer) будет плюсом.

Критерии оценки (штрафы суммируются при наличии нескольких ошибок):

• Дерево создано, но сертификаты не собраны в PKCS - минус 2 балла

• Дерево сертификатов создано, но отображается в Windows с ошибкой в одном сертификате - минус 2 балла

• Дерево сертификатов создано, но отображается в Windows с ошибками более чем в одном сертификате - всего 0 баллов

• Использованы другие расширения или не использованы требуемые - минус 2 балла

• При создании сертификата требуется ввод информации с клавиатуры (всё должно работать автоматически!) - минус 1 балла

• Поля Субъект (Subject) и Издатель (Issuer) заполнены по английским — минус 1 балл.

СЗИ №2

Трафик к веб-сервисам станции должен быть защищен от перехвата. Давайте потренируемся. Создайте с помощью OpenSSL цифровой сертификат и примените его для создания защищенной связи по протоколу HTTPS с веб-сервером на Вашей виртуальной машине. Веб-сервер (если не запущен) запустите самостоятельно.

Итог работы. Загрузите в предоставленные формы 5 файлов:

• Скриншот (в формате .png, пример ниже) установления защищенного доступа по протоколу HTTPS к веб-серверу с хост-машины (ПК участника) при открытом цифровом сертификате

• Скриншот (в формате .png, пример ниже) установления защищенного доступа по протоколу HTTPS к веб-серверу с хост-машины (ПК участника)

• Созданный сертификат

• Скрипт OpenSSL для создания сертификата (zip-архив в случае нескольких файлов)

• Конфигурационные файлы веб-сервера, в которые внесены изменения (zip-архив в случае нескольких файлов)

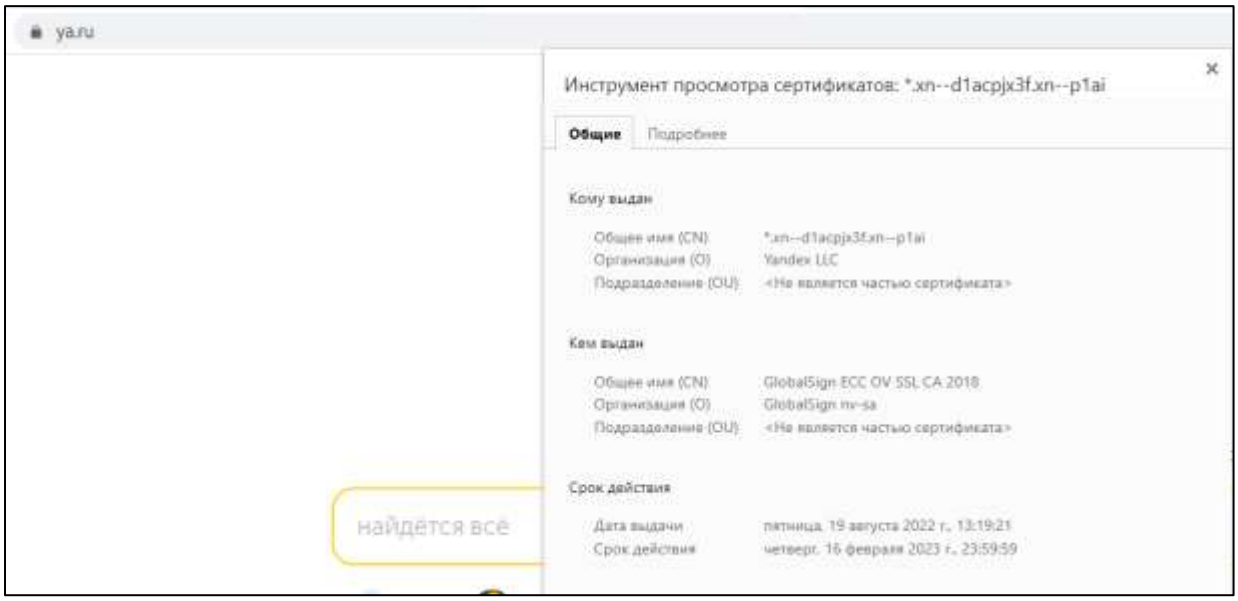

Рисунок 2 - пример защищенного соединения по протоколу HTTPS (с сайтом Яндекса) — обратите внимание на символ замка, обозначающий безопасное соединение. В цифровом сертификате должны быть читаемы все поля: должно быть понятно, что сертификат создан участником

Критерии оценки (штрафы суммируются при наличии нескольких ошибок):

Все файлы должны быть предоставлены, на скриншоте должно быть видно установленное соединение по HTTPS без ошибок. В поле Subject (Общее имя, Субъект) сертификата должно совпадать с URL веб-сервера (IP адресом или доменным именем). Если замочек HTTPS отсутствует— ноль баллов. Если есть следы подделки (не совпадают данные по сертификату в скрипте и конечном сертификате и т.п.) — ноль баллов