

Инструкция участника проектного тура

Тематики заданий

В туре необходимо решить как можно больше заданий. Наборы заданий ориентированы на комплексную оценку навыков участников заключительного этапа и охватывают темы:

1. Reverse/PWN - Реверс-инжиниринг (анализ исходных текстов компьютерных программ)
2. Web (поиск уязвимостей веб-приложений)
3. Forensics (поиск следов инцидентов информационной безопасности)
4. Privesc/Misc - Linux\Unix (Misc) (задания смешанной категории, защита ОС Linux\Unix)
5. Crypto - Криптография
6. СЗИ - Средства защиты информации
7. Network - Защита сетей связи

Важные условия

Оценка заданий (включая тематику СЗИ) производится автоматически по факту размещения участником в поле для ввода корректного флага (ответа) – строки определенного вида, доступ к которому является индикатором успешного решения задания.

Максимально возможное число баллов за практический тур – 70 баллов.

Техническая инструкция для участника приведена ниже.

Перед началом тура участникам выделено время на ознакомление данной инструкцией, расположением файлов со справочными материалами (т.н. manuals & hack tricks) на машине участника, на проверку доступности с виртуальной машины участника платформы ctfd.

Учетные данные для входа в ВМ участника - kali/kali. Учетные данные для ctfd выдаются в индивидуальном порядке и не могут передаваться между участниками.

Инфраструктура

1. На ПК участника олимпиады должен отсутствовать доступ в сеть “Интернет”, исключение - доступ к VPN платформы, в случае удаленного участия.
2. На ПК участника установлен гипервизор VirtualBox¹.
3. Участнику предоставлен образ виртуальной машины с необходимым программным обеспечением для решения заданий. Виртуальную машину (ВМ) участника требуется запустить до начала практического тура и выполнить тестовый вход на платформу. Тестовые учетные записи предоставляются отдельно. ВМ участника включает:
 - Необходимый набор утилит для решения задач практической части.
 - README.txt с их перечнем.
 - Cheatsheet (инструкции) с информацией по вариантам использования инструментария.
4. На сервере организаторов запущена виртуальная машина с Платформой с заданиями (т.н. решающая система), доступная по локальной сети с машин участников.

Порядок проведения

Длительность практического тура составляет **5 часов**. В случае обнаружения неисправности в оборудовании, возникшей не по вине участника, по решению Организаторов, данный участник может пересест на резервный ПК. Время, затраченное на устранение такой неисправности, компенсируется. Вредоносное воздействие участником на инфраструктуру площадки (вывод из строя оборудования, ПО и т.п.) влечет дисквалификацию на проектный тур целиком.

Общие требования

1. Задания, файлы, приложения для выполнения заданий расположены на Платформе CTFd на сервере организаторов. Участники получают персональный логин и пароль доступа.
2. Участники выполняют задания полностью самостоятельно. Задания расположены на Платформе. Необходимый программный инструментарий для их решения есть на виртуальных машинах на ПК участников.
3. По окончании решения заданий участник олимпиады может покинуть аудиторию.
4. Найденные флаги вводятся на Платформе. Если количество попыток ввода флага ограничено, это указано в тексте задания. Успешно найденный флаг в поисковых задачах обычно имеет формат **vsosh{}**, если это не оговорено в задании отдельно (обычно в заданиях типа Network, СЗИ и т.п.).
5. В некоторых заданиях содержится несколько флагов (т.е. для одного текста/файлов задания доступно несколько флагов для поиска). В этом случае каждый флаг сдаётся на платформе CTFd отдельно (по соответствующей кнопке). Что является флагами определено в задании.

¹ <https://www.virtualbox.org/wiki/Downloads>

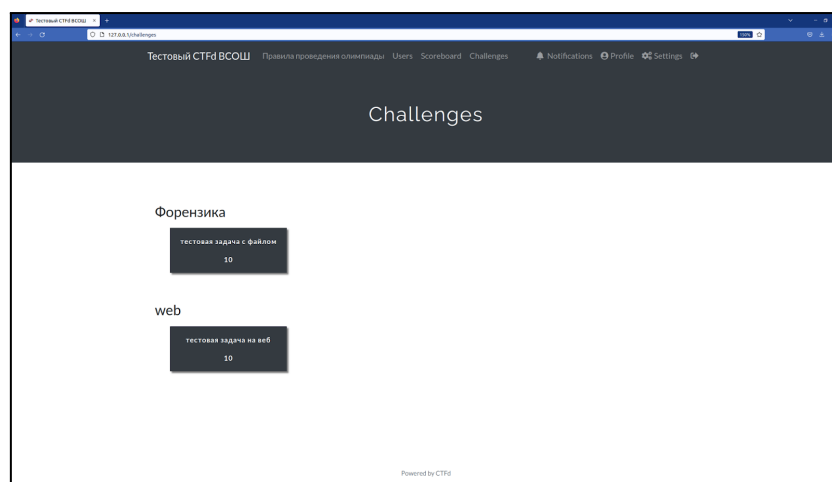


Рисунок 1 – примерный вид экранного интерфейса Платформы с заданиями

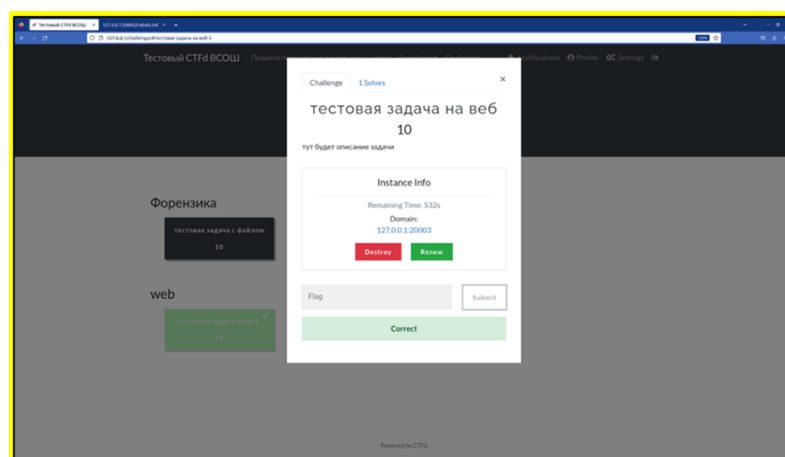
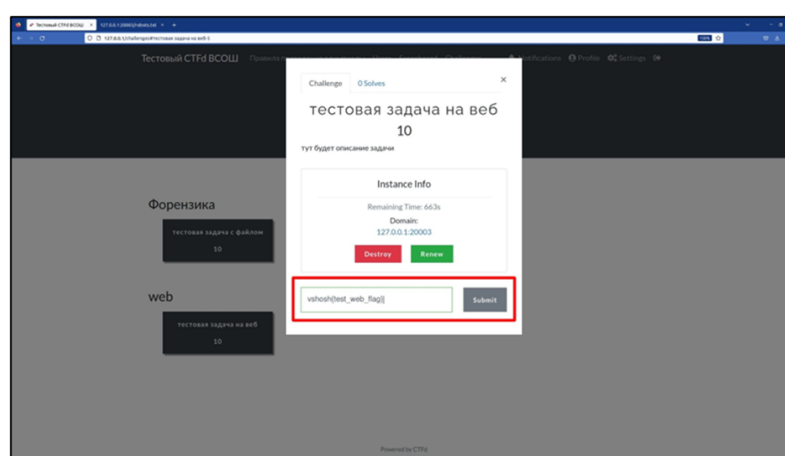


Рисунок 2 – пример успешного ввода флага. Задание засчитано.

Техническая информация

> [H3ll0, W0r1d]

Добрый день, участник заключительного этапа!

В рамках практического тура сегодня тебе предстоит выполнить как можно больше заданий из представленных на платформе. Заметь задания СЗИ теперь также сдаются на платформе.

В рамках ограничений по времени и отсутствия подключения к Сети, мы традиционно предоставляем документацию - `hacktricks`, `OWASP CheatSheetSeries` и `PayloadAllTheThings`, клонированные репозитории расположены на рабочем столе:

```
/home/kali/Desktop/hacktricks  
/home/kali/Desktop/CheatSheetSeries  
/home/kali/Desktop/PayloadAllTheThings
```

Для удобства, был установлен reader md файлов - `Obsidian` и редактор кода `VScode` с плагинами `pylance` и `cvs table` (при просмотре cvs файла, справа сверху появляется иконка для активации плагина).

С этими утилитами удобно читать документацию.

> [REMINDER]

Путь до `rockyou.txt` :

```
/usr/share/wordlists/rockyou.txt
```

> [REMINDER]

Также для удобства решения некоторых заданий, мы установили несколько дополнительных утилит:

> [INFO] : Дополнительно установленные утилиты:

- Ghidra
- IDA Freeware 9.2
- gdb
- edb
- strace
- ltrace
- dirsearch
- go
- curl
- Libreoffice
- binwalk
- vscode

- jadx
- volatility
- patchelf
- ropgadget
- one_gadget

> [INFO] : Дополнительно установленные расширения gdb:

- pwndbg
- gef - чтобы им воспользоваться, необходимо раскомментировать строку модуля в /home/kali/.gdbinit и закомментировать pwn

> [INFO] : Дополнительно установленные модули Python 3:

- pwntools, ipython3, pycryptodome, pybase64, sympy

> [INFO] : Дополнительно установленные расширения BurpSuite:

- JWT Editor

> [INFO] : Jadx folder:

/home/kali/jadx-1.5.5/bin

> [INFO] : Volatility folder:

/home/kali/volatility3-2.27.0

> [INFO] : Вспомогательные материалы к заданию категории СЗИ доступны по пути:

/home/kali/Desktop/CheatSheetSeries
Их также удобно читать в Obsidian

P.S.

Внимательно читайте описание и название заданий, это сэкономит время их решения!
Следите за числом попыток сдачи и не забывайте о наличии документации, она добавлена не случайно!).

Памятка по быстрым клавишам.

- ctrl+F - переключение режима экрана VirtualBox (в случае проблем с разрешением).
- F12 - разрешить вставку команд в консоль разработчика Firefox