Информация для организаторов
регионального этапа всероссийской олимпиады
школьников по информатике 2025 – 2026 учебный год
Профиль “Информационная безопасность”, 10 класс

Данная страница предназначена для организаторов регионального этапа и участникам не выдаётся!

Детальные инструкции организаторам предоставляются на почту председателя жюри регионального этапа!

Виртуальные машины для выполнения задания и инструкции по развертыванию доступны для скачивания в сети Интернет во время проведения Олимпиады по ссылкам ниже:

Основная ссылка: https://miem.hse.ru/rosh/2026

Резервная ссылка: https://vsosh.miem.hse.ru/organizers

Логины и пароли от административного интерфейса виртуальных машин предоставляются председателю жюри (или назначенному ответственному лицу) региональным операторам ВСОШ за 4 суток до проведения олимпиады.

Практическое задание для регионального этапа всероссийской олимпиады школьников по технологии 2025 – 2026 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 регионального тура и охватывают перечисленные ниже 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 – строки определенного вида (шаблон будет озвучен перед началом тура), доступ к которому является индикатором успешного решения задания.

Максимально возможное число баллов за практический тур – 70 баллов.

Инструкция для участника приведена ниже, перед заданием.

Перед началом тура участники должны быть ознакомлены с инструкцией и расположением файлов с инструкциями (т.н. manuals & hack tricks) на машине участника, проверить доступность с виртуальной машины участника платформы ctfd.

Время на ознакомление с машиной изучение этих документов (до 30 минут) не входит в общее время выполнения заданий.

Общая длительность тура указана в документе “Требования к организации и проведению регионального этапа всероссийской олимпиады школьников в 2025/26 учебном году”.

Инструкция для администраторов (организаторов этапа) распространяется отдельно, является конфиденциальной и участникам не предоставляется.

Инструкция участника

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 должен быть установлен гипервизор VirtualBox[1].
3. Участнику предоставляется 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. Обязательно отсутствие у участника Административных прав в хост-системе. 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. В случае удаленного участия, необходима организация VPN доступа (инструкция предоставляется отдельно) до Платформы проведения. В случае локального проведения, на сервере организаторов запускается виртуальная машина с Платформой с заданиями (т.н. решающая система). Виртуальная машина с Платформой должна быть доступна по локальной сети с машин участников.
5. До начала выполнения заданий все участники должны быть зарегистрированы на Платформе CTFd и получить логин/пароль.

Порядок проведения

Длительность практического тура (выполнение практических заданий) для участников 9 класса составляет: не менее **5 часов** (без учета перерывов). В случае обнаружения неисправности в оборудовании, возникшей не по вине участника, по решению Организаторов данный участник может пересесть на резервный ПК. Время, затраченное на устранение такой неисправности, компенсируется.

Общие требования

1. До начала практического тура необходимо обеспечить доступ с ПК участников к Платформе с заданиями. Участники получают персональный логин и пароль доступа.
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.

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

4. Найденные флаги вводятся на Платформе. Если количество попыток ввода флага ограничено, это указано в тексте задания. Успешно найденный флаг в поисковых задачах имеет обычно формат vsosh{} ,если это не оговорено в задании отдельно (обычно в заданиях типа Network, СЗИ, Форензика).

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.

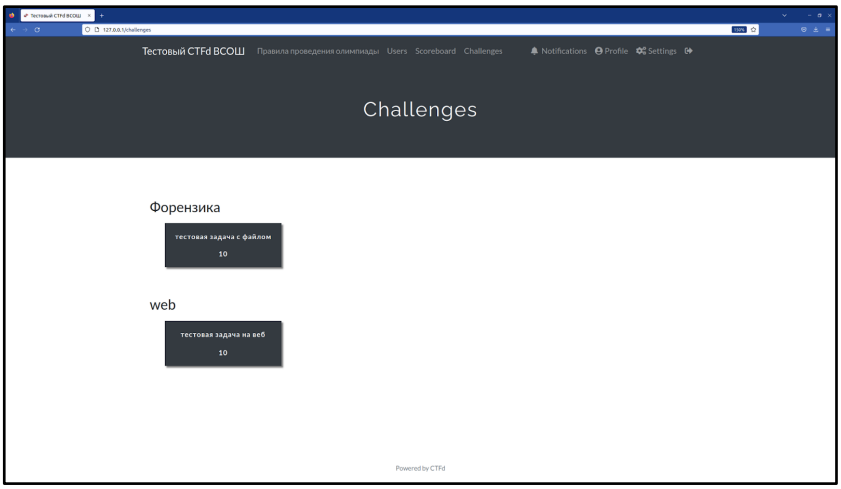
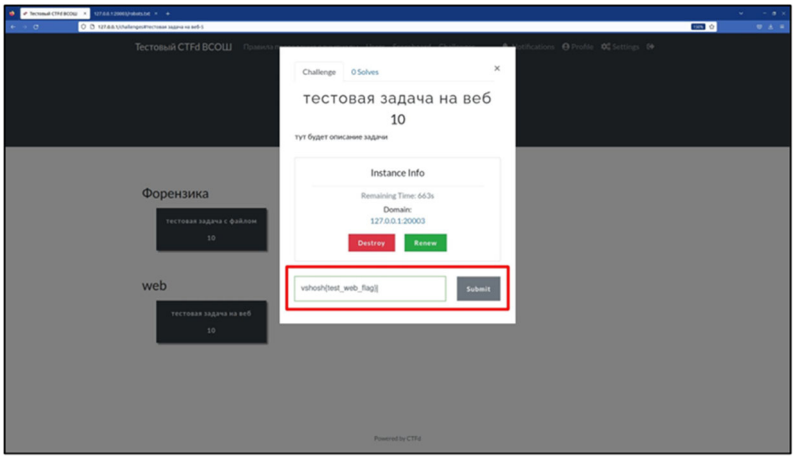


Рисунок 1 – примерный вид экранного интерфейса Платформы с заданиями



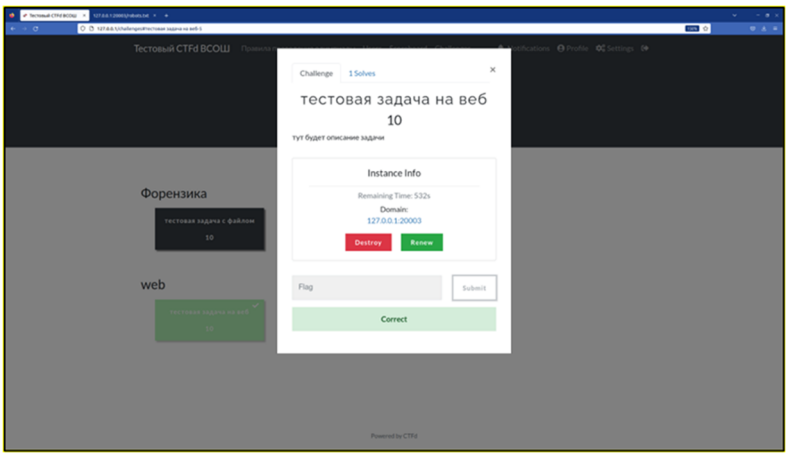


Рисунок 2 – пример успешного ввода флага. Задание засчитано.

Технические детали и утилиты

> [H3ll0, W0r1d]

Добрый день, участник регионального этапа!
В рамках практического тура сегодня тебе предстоит
выполнить как можно больше заданий из представленных на платформе.

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

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

Для твоего удобства установлен reader md файлов - Obsidian.
Открой его, чтобы с удобством 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

> [INFO] : Дополнительно установленные расширения gdb:

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

> [INFO] : Дополнительно установленные модули Python 3:

- pwntools, pybase64, sympy

> [INFO] : Дополнительно установленные расширения BurpSuite:

- JWT Editor

> [INFO] : Volatility folder:

/home/kali/volatility3
При использовании volatility3 надо активировать виртуальное окружение - source /home/kali/volatility3/venv/bin/activate

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

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

> [G00d Luck]

Сеттинг этого года – Хакеркрафт, вселенная про блоки, крафт и таинственные загадки.

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!

Карта разбалловки для 10 классов

№ Задания	Тематика задания	Критерии оценки	Кол-во баллов
1.	**Crypto-1**	Факт размещения участником в поле для ввода 1 корректного флага	2
2.	**Web-1**	Факт размещения участником в поля для ввода 2 корректных флагов	1+3
3.	**Web-2**	Факт размещения участником в поля для ввода 2 корректных флагов	2+4
4.	**Network-1**	Факт размещения участником в поля для ввода 3 корректных флагов	2+2+2
5.	**Forensics-1**	Факт размещения участником в поля для ввода 3 корректных флагов	1+2+2
6.	**Forensics-2**	Факт размещения участником в поля для ввода 2 корректных флагов	2+3
7.	**Reverse-1**	Факт размещения участником в поле для ввода 1 корректного флага	3
8.	**Reverse-2**	Факт размещения участником в поля для ввода 2 корректных флагов	2+5
9.	**PWN-1**	Факт размещения участником в поле для ввода 1 корректного флага	1+7
10.	**СЗИ-1**	Факт размещения участником в поле для ввода 1 корректного флага	4
11.	**СЗИ-2**	Факт размещения участником в поля для ввода 5 корректных флагов	1+1+1+1+1=5
12.	**Crypto-2**	Факт размещения участником в поле для ввода 1 корректного флага	6
13.	**Privesc-1**	Факт размещения участником в поле для ввода 1 корректного флага	5
14.	**Misc-1**	Факт размещения участником в поля для ввода 2 корректных флагов	1+3
Σ			**70**

Задания 10 КЛАСС

Окунись в волшебный мир ХакерКрафта! Вооруженный знаниями и специальным инструментарием защити Верхний мир от угроз информационной безопасности – решай задачи и получай баллы за каждый верный ответ!

Crypto-1 – Тайна пиглинов (1/1)

В ходе долгих странствий добыта табличка с координатами бастиона пиглинов. Понятно, зашифрованными. В ходе допроса брутального командира пиглинов на вопрос “что это за шифр?” он хрюкал что-то вроде openssl enc -ae… -K ...и дальше неразборчиво. Понятно, что свой шифр пиглины придумать не в состоянии, и пользуются какими-то стандартными средствами. Надо получить координаты бастиона!

Рекомендуемые утилиты: openssl, bash и др.
Цель работы: получение доступа к флагу.
Критерий оценки: предоставление правильного флага.

Рекомендуемые утилиты: openssl, bash и др.
Цель работы: получение доступа к флагу.
Критерий оценки: предоставление правильного флага.

Web-1 - Заброшенный бастион (1/2)

На поверхности, рядом с не зажженным порталом в Незер, стоит табличка с выцветшей надписью и нарисованным Визером. Кажется, послание для внимательных путешественников записано прямо на одной из нескольких голов Визера.

Рекомендуемые утилиты: burp suite, curl и др.
Цель работы: Найти флаг, изучив ответы сервера
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление корректного флага.

Web-1 - Заброшенный бастион (2/2)

Наконец, мы смогли зажечь портал и попасть в Незер, где сразу же увидели заброшенный бастион. У входа в бастион кто-то прибил две таблички — «static» и «secret/flag.txt». Доски сгнили, а каменная кладка треснула — кажется, если идти назад по тропе слишком далеко, можно шагнуть за ограждение и попасть туда, куда не должны.

Рекомендуемые утилиты: burp suite, curl и др.
Цель работы: Добраться до защищённого тайника и найти флаг
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление корректного флага.

Web-2 - Обмани жителя (1/2)

Жители этой деревни хранят страшные тайны, скрывая их от посторонних. Но мы уверены, что именно ты сможешь раскрыть их. Для начала узнай, что староста обсуждал с ведьмой.

Рекомендуемые утилиты: burp suite, Python и др.
Цель работы: получить доступ к личным сообщениям пользователя «замстаросты»
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление корректного флага.

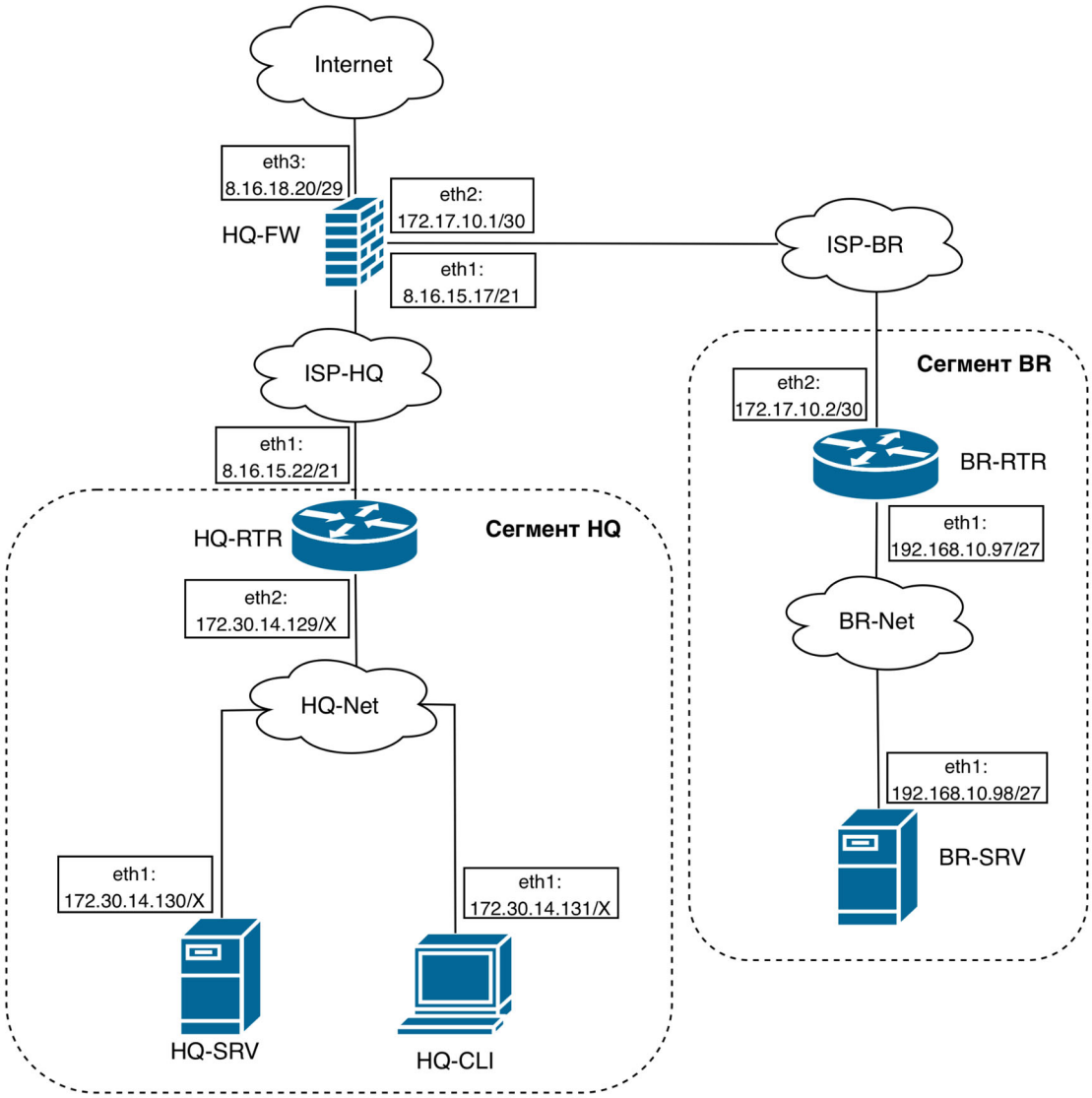
Web-2 - Обмани жителя (2/2)

Жители этой деревни хранят страшные тайны, скрывая их от посторонних. Но мы уверены, что именно ты сможешь раскрыть их. Время извлечь тайные знания.

Рекомендуемые утилиты: burp suite, Python, curl и др.
Цель работы: вручную извлечь флаг из базы данных
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление корректного флага.

Network -1 – сети (1/3)

На изображении представлена схема сети. На основе этой схемы ответьте на вопросы.



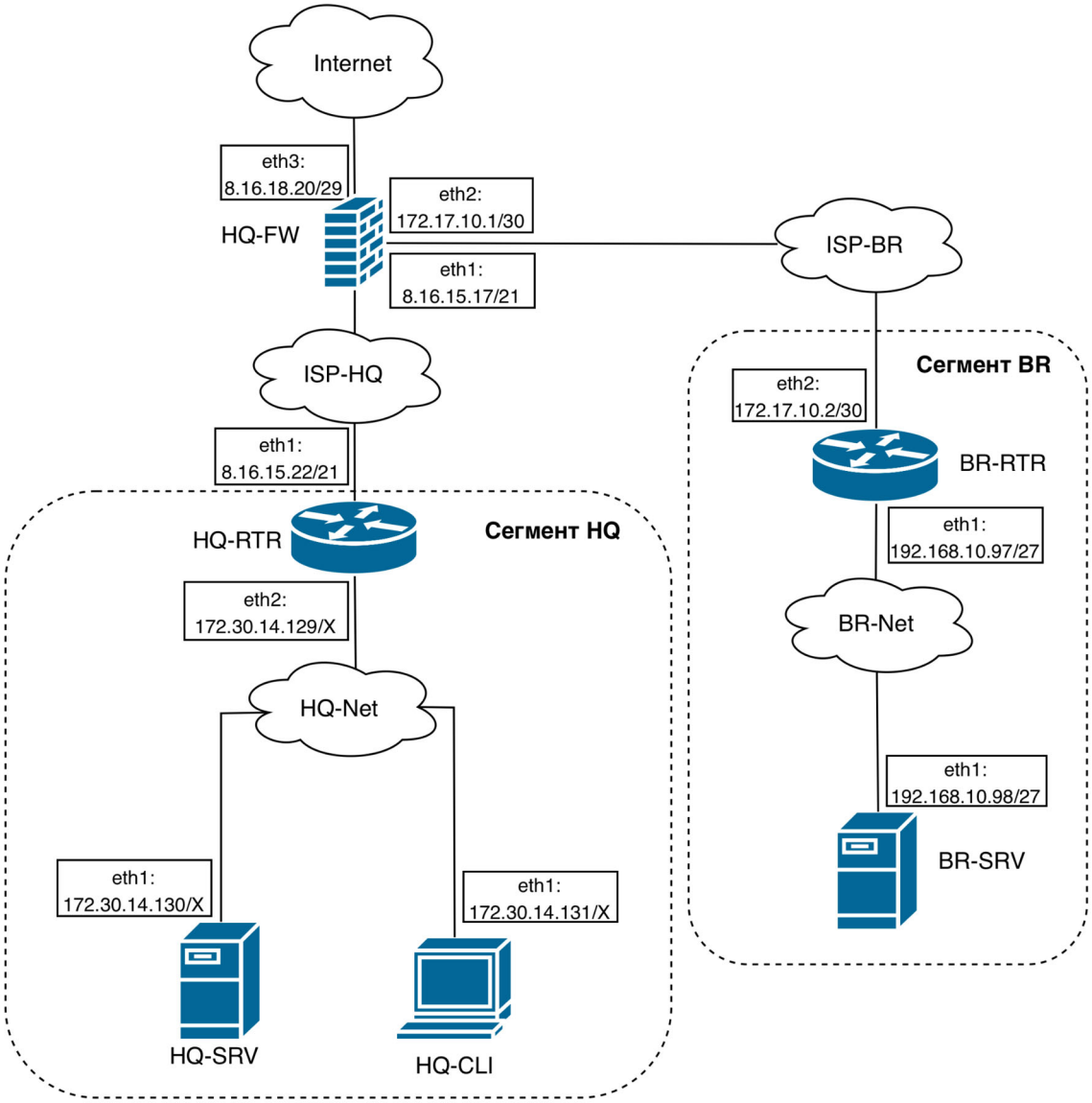
Какая максимальная длина префикса сети, которую можно задать для подсети HQ-Net, чтобы все её узлы оставались в одной подсети? В ответ запишите только число (например, 24).

ВАЖНО: Вопрос имеет ограниченное число неудачных попыток - только **1 попытка** ответа на вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: текстовый редактор и др.
Цель работы: ответить на вопрос задания
Итог работы: корректно вписать ответ
Критерий оценки: предоставление корректного ответа

Network -1 – сети (2/3)

На изображении представлена схема сети из предыдущего задания. На основе этой схемы ответьте на вопросы.



Нужно настроить преобразование адресов для всей внутренней подсети BR-Net (192.168.10.96/27) в целях обеспечения доступа в Интернет. Какое правило iptables нужно добавить на BR-RTR?

iptables -t <ПАРАМЕТР1> -A POSTROUTING -s 192.168.10.96/27 -o <ПАРАМЕТР2> -j <ПАРАМЕТР3>

Выберете пропущенные параметры и объедините их в ответ (флаг) в следующем виде, через разделитель “_”:

ПАРАМЕТР1_ПАРАМЕТР2_ПАРАМЕТР3

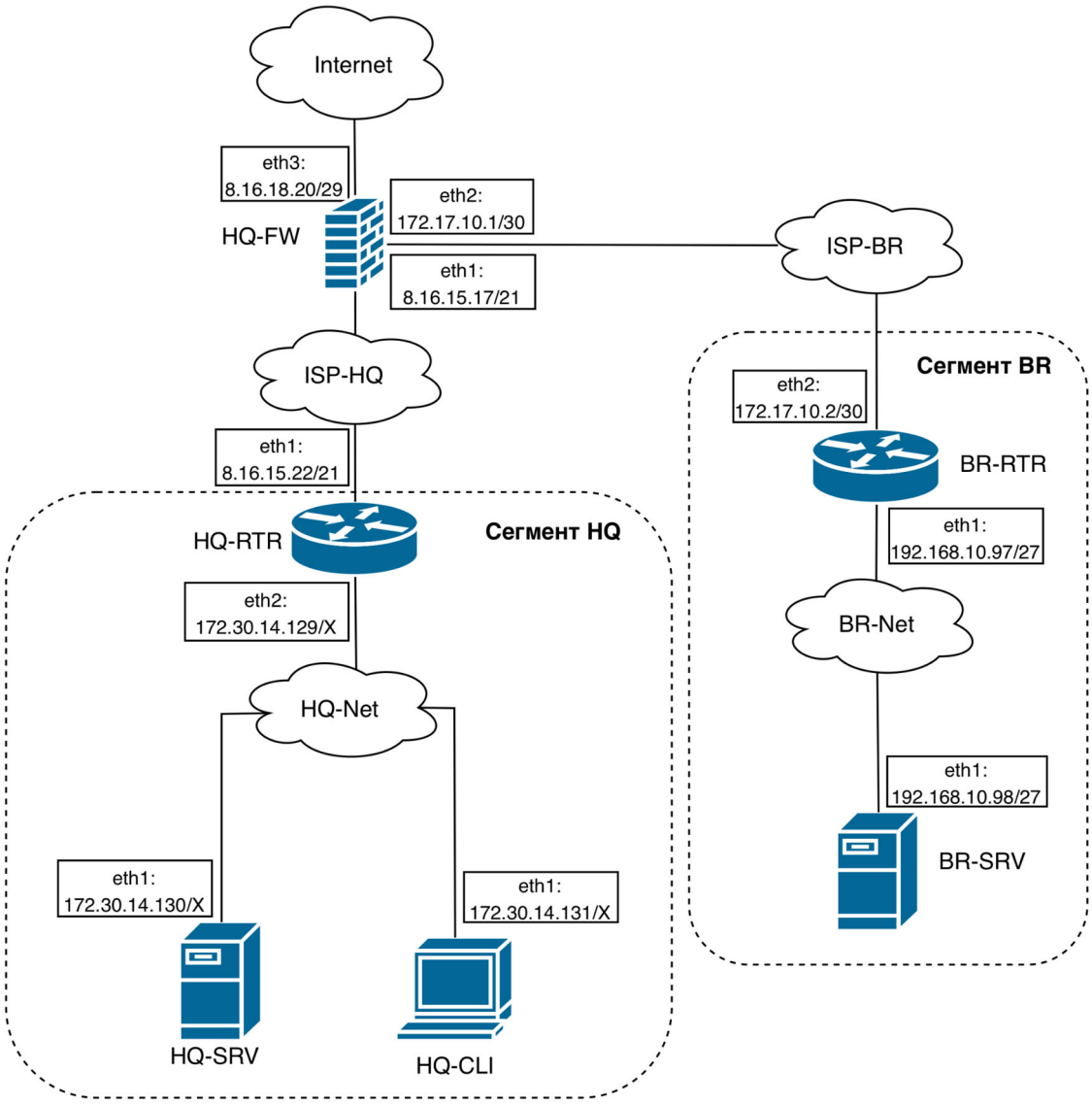
Например, если ПАРАМЕТР1 = SEND, ПАРАМЕТР2 = ++tuda, ПАРАМЕТР3 = 2026 то итоговый флаг будет SEND_++tuda_2026

ВАЖНО: Ответы представленные в другом виде или с ошибкой хотя бы в одном символе приняты к ответу не будут. Вопрос имеет ограниченное число неудачных попыток - только **2 попытки** ответа на вопрос! Ответ нужно сдавать без обертки vsosh{...}.

Рекомендуемые утилиты: текстовый редактор и др.
Цель работы: ответить на вопрос задания
Итог работы: корректно вписать ответ
Критерий оценки: предоставление корректного ответа

Network -1 – сети (3/3)

На изображении представлена схема сети из предыдущего задания. На основе этой схемы ответьте на вопросы.



Какая комбинация аргументов позволяет задать маршрут по-умолчанию на BR-RTR для обеспечения маршрутизации в сегмент HQ? Введите в поле ответа номер варианта (число 1, 2, 3, 4 или 5)! Варианты ответа:

1. route add 0.0.0.0 mask 0.0.0.0 via eth2

2. route add 0.0.0.0 mask 0.0.0.0 via 172.17.10.2

3. route add default gw 172.17.10.1

4. route add default gw 8.16.18.20

5. route add new default gw 8.16.18.20

ВАЖНО: Вопрос имеет ограниченное число неудачных попыток - только 2 **попытки** ответа на вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: текстовый редактор и др.
Цель работы: ответить на вопрос задания
Итог работы: корректно вписать ответ
Критерий оценки: предоставление корректного ответа

Forensics 1: Вредоносный мод-пак (1/3)

На популярном форуме игроков распространялся "оптимизированный" мод-пак для увеличения FPS. После установки у игроков начали пропадать вещи из сундуков. У Вас есть архив с модами и логи клиента одной из жертв. Найдите вредоносный мод и его функционал.

Флаг **№1** необходимо сдать в формате: ***Название Java-файла с вредоносным модом***. Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: unzip, jar, grep, strings и др.
Цель работы: анализ модификаций игры, поиск бэкдоров
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 1: Вредоносный мод-пак (2/3)

На популярном форуме игроков распространялся "оптимизированный" мод-пак для увеличения FPS. После установки у игроков начали пропадать вещи из сундуков. У Вас есть архив с модами и логи клиента одной из жертв. Найдите вредоносный мод и его функционал.

Флаг **№2** необходимо сдать в формате: ***Порт, на который мод отправляет данные.*** Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: unzip, jar, grep, strings и др.
Цель работы: анализ модификаций игры, поиск бэкдоров
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 1: Вредоносный мод-пак (3/3)

На популярном форуме игроков распространялся "оптимизированный" мод-пак для увеличения FPS. После установки у игроков начали пропадать вещи из сундуков. У Вас есть архив с модами и логи клиента одной из жертв. Найдите вредоносный мод и его функционал.

Флаг **№3** необходимо сдать в формате: *vsosh{**Команду, которую мод выполняет скрытно от игрока***}, то есть ответ обернуть в форму *vsosh{}*. Если аргументы/составные части команды передаются через пробел, то в ответе запишите саму команду без косой черты, а пробелы через нижнее подчеркивание ("_"). Пример: “/echo i love cats 22” --> “echo_i_love_cats_22”.

Рекомендуемые утилиты: unzip, jar, grep, strings и др.

Цель работы: анализ модификаций игры, поиск бэкдоров
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 2: Поврежденная карта мира (1/2)

После внезапного отключения электричества главный мир сервера "CraftWorld" перестал загружаться. Бэкапы оказались повреждены. У Вас есть образ диска сервера. Восстановите важные данные и найдите координаты тайной базы администратора, где хранятся все ресурсы для ивентов.

Флаг **№1** необходимо сдать в формате: ***IP-адрес последнего администратора, который подключался к серверу.*** Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: mount, losetup, strings, grep и др.
Цель работы: исследование образа диска, восстановление удаленных файлов
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 2: Поврежденная карта мира (2/2)

После внезапного отключения электричества главный мир сервера "CraftWorld" перестал загружаться. Бэкапы оказались повреждены. У Вас есть образ диска сервера. Восстановите важные данные и найдите координаты тайной базы администратора, где хранятся все ресурсы для ивентов.

Флаг **№2** необходимо сдать в формате: ***Координаты секретной базы из поврежденного текстового файла***. Формат указания координат для флага - через нижнее подчеркивание вместо пробелов: X_Y_Z. Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: losetup, strings, grep и др.
Цель работы: исследование образа диска, восстановление удаленных файлов
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Reverse 1 – Редстоуновый механизм (1/1)

В заброшенной крепости ты нашел сундук, защищенный сложным редстоуновым механизмом. Рядом с каждым рычагом стоит табличка со странными символами и числами. Изучи схему и найди правильную последовательность, чтобы активировать remote-механизм и открыть сундук с алмазами!

Рекомендуемые утилиты: python, gcc и др.
Цель работы: Восстановить пароль и подключившись к серверу, получить флаг.
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Reverse 2 - Командный блок (1/2)

На заброшенном сервере Minecraft был найден странный файл — зашифрованная команда из командного блока. Программа command_block.elf — это древний инструмент администраторов для шифрования секретных команд. Используй свои навыки reverse engineering, чтобы восстановить оригинальную команду и найти ключ активации!

Рекомендуемые утилиты: Ghidra, Python и др.

Цель работы: Найти ключ шифрования

Итог работы: Получить доступ к первому флагу
Критерий оценки: предоставление правильного флага.

Reverse 2 - Командный блок (2/2)

На заброшенном сервере Minecraft был найден странный файл — зашифрованная команда из командного блока. Программа command_block.elf — это древний инструмент администраторов для шифрования секретных команд. Используй свои навыки reverse engineering, чтобы восстановить оригинальную команду и найти ключ активации!

Рекомендуемые утилиты: Ghidra, Python и др.

Цель работы: Расшифровать команду

Итог работы: Получить доступ ко второму флагу.
Критерий оценки: предоставление правильного флага.

PWN 1: Портал в Край (1/2)

Ты наткнулся на древний портал в Край, но что-то пошло не так!

Портал мерцает странными символами и явно работает некорректно. Рядом лежит потрёпанная книга с надписью "Руководство администратора портала".

Листая страницы, ты находишь записи о том, что портал был создан древними строителями и имел систему защиты от несанкционированного доступа.

Но время не пощадило конструкцию - многие защитные механизмы давно вышли из строя.

Похоже, это твой единственный шанс добраться до сокровищницы Края...

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

Цель работы: поиск и эксплуатация уязвимости в бинарном приложении

Итог работы: получить доступ ко первому флагу.
Критерий оценки: предоставление правильного флага.

PWN 1: Портал в Край (2/2)

Ты наткнулся на древний портал в Край, но что-то пошло не так!

Портал мерцает странными символами и явно работает некорректно. Рядом лежит потрёпанная книга с надписью "Руководство администратора портала".

Листая страницы, ты находишь записи о том, что портал был создан древними строителями и имел систему защиты от несанкционированного доступа.

Но время не пощадило конструкцию - многие защитные механизмы давно вышли из строя.

Похоже, это твой единственный шанс добраться до сокровищницы Края...

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

Цель работы: поиск и эксплуатация уязвимости в бинарном приложении

Итог работы: получить доступ ко второму флагу.

Критерий оценки: предоставление правильного флага.

СЗИ 1 - Защита от грифера (1/1)

Гриферы взломали сайт с покупкой лицензий Майнкрафта. Почини форму входа так, чтобы гриферы тоже платили, а не играли за чужой счет.

Рекомендуемые утилиты: python (помни, стажёр, про число пробелов в операторах в python) и др.

Цель работы: изменение кода приложения.

Итог работы: получить флаг после верного исправления кода.

Критерий оценки: предоставление правильного флага.

СЗИ 2 - Деревенский сыщик (1/5)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но служба установки java-ядра мира оказалась захвачена и разорена. Наблюдатель уловил все события атаки на деревню, но он не смог ничего объяснить, только предоставил диск с записью. Вставь его в проигрыватель CSV и ответь на все вопросы задания.

Какой вредоносный файл загрузил и запустил пользователь? Укажите полную ссылку, по которой был загружен файл.

ВАЖНО: Задание разбито на несколько отдельных вопросов, доступных в едином файле. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют **ограниченное число неудачных попыток - по 3 попытки** ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, текстовый редактор и др.

Цель работы: исследование вредоносной активности в записи логов и сдача ответов на платформе

Итог работы: Получить ответы на 5 вопросов

Критерии оценки: предоставление правильных ответов

СЗИ 2 - Деревенский сыщик (2/5)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но служба установки java-ядра мира оказалась захвачена и разорена. Наблюдатель уловил все события атаки на деревню, но он не смог ничего объяснить, только предоставил диск с записью. Вставь его в проигрыватель CSV и ответь на все вопросы задания.

С помощью какого вредоносного скрипта злоумышленник произвел разведку? Укажите название скрипта с расширением.

ВАЖНО: Задание разбито на несколько отдельных вопросов, доступных в едином файле. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют **ограниченное число неудачных попыток - по 3 попытки** ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, текстовый редактор и др.

Цель работы: исследование вредоносной активности в записи логов и сдача ответов на платформе

Итог работы: Получить ответы на 5 вопросов

Критерии оценки: предоставление правильных ответов

СЗИ 2 - Деревенский сыщик (3/5)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но служба установки java-ядра мира оказалась захвачена и разорена. Наблюдатель уловил все события атаки на деревню, но он не смог ничего объяснить, только предоставил диск с записью. Вставь его в проигрыватель CSV и ответь на все вопросы задания.

С помощью какой службы были повышены привилегии?

ВАЖНО: Задание разбито на несколько отдельных вопросов, доступных в едином файле. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют **ограниченное число неудачных попыток - по 3 попытки** ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, текстовый редактор и др.

Цель работы: исследование вредоносной активности в записи логов и сдача ответов на платформе

Итог работы: Получить ответы на 5 вопросов

Критерии оценки: предоставление правильных ответов

СЗИ 2 - Деревенский сыщик (4/5)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но служба установки java-ядра мира оказалась захвачена и разорена. Наблюдатель уловил все события атаки на деревню, но он не смог ничего объяснить, только предоставил диск с записью. Вставь его в проигрыватель CSV и ответь на все вопросы задания.

Приведите логин и пароль с которым злоумышленник перескочил на второй хост? Укажите логин:пароль.

ВАЖНО: Задание разбито на несколько отдельных вопросов, доступных в едином файле. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют **ограниченное число неудачных попыток - по 3 попытки** ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, текстовый редактор и др.

Цель работы: исследование вредоносной активности в записи логов и сдача ответов на платформе

Итог работы: Получить ответы на 5 вопросов

Критерии оценки: предоставление правильных ответов

СЗИ 2 - Деревенский сыщик (5/5)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но служба установки java-ядра мира оказалась захвачена и разорена. Наблюдатель уловил все события атаки на деревню, но он не смог ничего объяснить, только предоставил диск с записью. Вставь его в проигрыватель CSV и ответь на все вопросы задания.

С помощью какой команды злоумышленник понял, какой утилитой надо повышать права на втором сервере?

ВАЖНО: Задание разбито на несколько отдельных вопросов, доступных в едином файле. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют **ограниченное число неудачных попыток - по 3 попытки** ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, текстовый редактор и др.

Цель работы: исследование вредоносной активности в записи логов и сдача ответов на платформе

Итог работы: Получить ответы на 5 вопросов

Критерии оценки: предоставление правильных ответов

Crypto 2: Сломанный стол зачарований (1/1)

Ты нашел в подземелье старый стол зачарований, но он работает неправильно! Вместо обычных зачарований он выдает зашифрованные руны.

Изучив механизм, ты понял: стол берет каждый символ заклинания, умножает его на уровень опыта игрока, добавляет количество лазурита в инвентаре, а результат ограничивает числом 256. К счастью, на столе есть табличка: "Все заклинания начинаются с vsosh{" - видимо, это стандартная магическая формула.

Сможешь ли ты взломать этот странный стол зачарований и получить настоящее заклинание?

Рекомендуемые утилиты: python, sympy

Цель работы: Расшифровать сообщение и получить флаг

Итог работы: Расшифрованное сообщение

Критерий оценки: Предоставление правильного флага

Privesc 1 - Бэкап карты (1/1)

На сервере каждую минуту автоматически создается резервная копия мира. Найди способ воспользоваться механизмом сохранения мира, чтобы узнать секретный сид!

Рекомендуемые утилиты: ssh, bash

Цель работы: Использовать систему бэкапов для получения прав администратора и прочитать флаг /root/flag.txt

Итог работы: получить доступ к флагу

Критерий оценки: Предоставление правильного флага

Misc 1 - Странный командный блок (1/2)

Гуляя по миру, вы нашли странный командный блок. Выяснилось, что он имеет доступ к хранилищу книг, и в одной из них есть секретные данные. Но вот беда - командный блок ограничивает количество команд.

Рекомендуемые утилиты: ssh

Цель работы: получить флаг не более, чем за пять команд

Итог работы: получить доступ к флагу

Критерий оценки: получение корректного флага

Misc 1 - Странный командный блок (2/2)

Гуляя по миру, вы нашли странный командный блок. Выяснилось, что он имеет доступ к хранилищу книг, и в одной из них есть секретные данные. Но вот беда - командный блок ограничивает количество команд, а секрет меняется после первой.

Рекомендуемые утилиты: ssh

Цель работы: получить флаг одной командой

Итог работы: получить доступ к флагу

Критерий оценки: получение корректного флага