Практическое задание для регионального этапа всероссийской олимпиады школьников по технологии 2025 – 2026 учебный год
Профиль “Информационная Безопасность”, 9 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.

Краткая 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.

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

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

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.

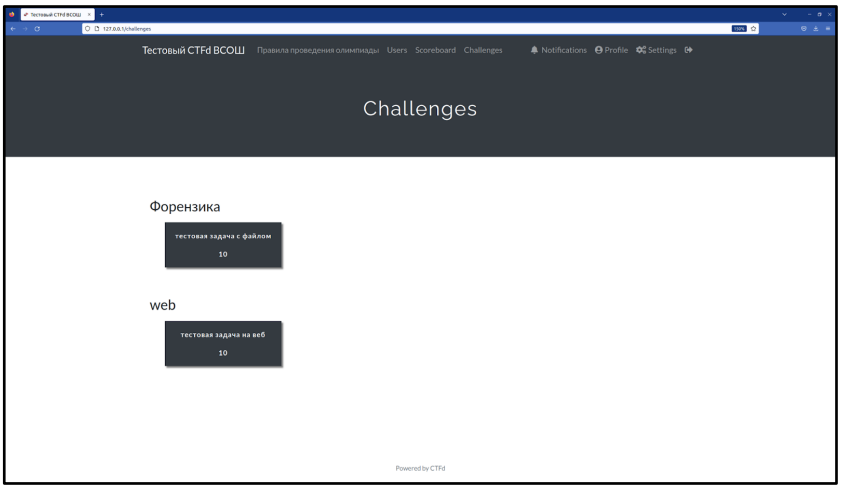
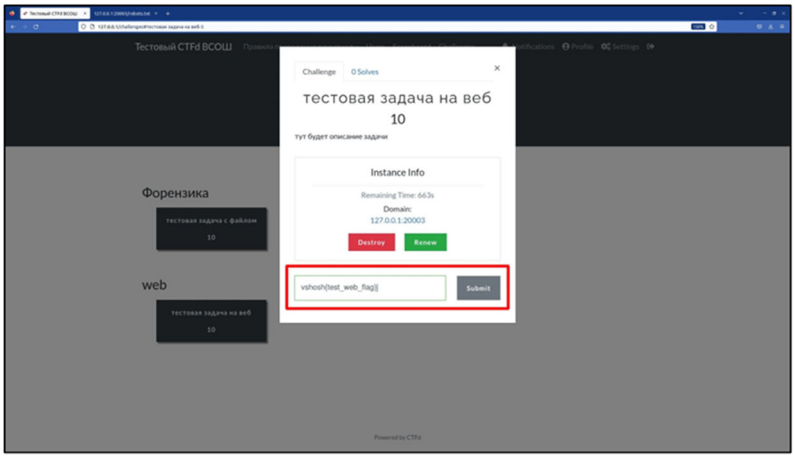


Рисунок 1 – примерный вид экранного интерфейса Платформы с заданиями



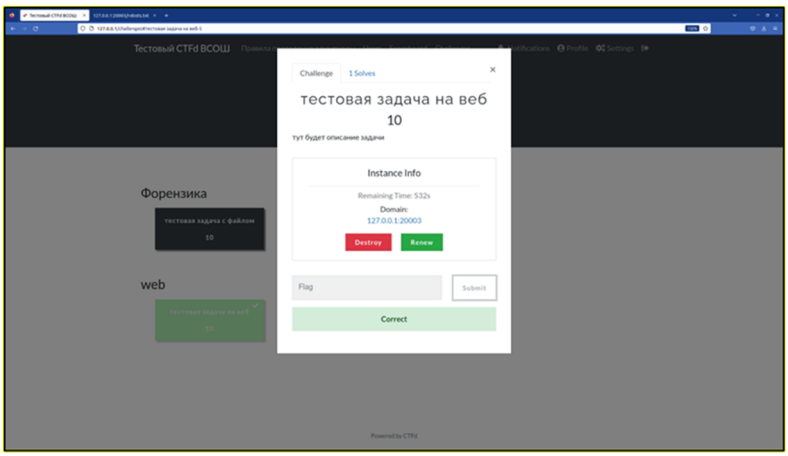


Рисунок 2 – пример успешного ввода флага. Задание засчитано.

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 9 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 поле для ввода 1 корректного флага	4
3.	**Web-2**	Факт размещения участником в поля для ввода 2 корректных флагов	2+4 = 6
4.	**Network-1**	Факт размещения участником в поля для ввода 3 корректных флагов	2+2+2 = 6
5.	**Forensics-1**	Факт размещения участником в поля для ввода 3 корректных флагов	1+2+2 = 5
6.	**Forensics-2**	Факт размещения участником в поля для ввода 2 корректных флагов	1+2+2
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 = 7
9.	**PWN-1**	Факт размещения участником в поле для ввода 1 корректного флага	1+7 = 8
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 9 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 странствий добыта табличка с координатами бастиона пиглинов. Понятно, зашифрованными. Чтобы разобраться “что это за шифр?” мы отловили и допросили брутального командира пиглинов. Он хрюкал что-то вроде openssl enc -des-ecb -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.

Web-1 - Ведьмина книга (1/1)

Говорят здесь можно найти рецепты зелий на любой вкус. Пролистайте ведьмину книгу и соберите удачное зелье.

Рекомендуемые утилиты: burp suite, Python и др.
Цель работы: анализ уязвимого web-приложения
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление корректного флага.

Web-2 - Зельеваренье (1/2)

В заброшенной лаборатории ты обнаружил варочную стойку с таинственным зельем. Исследуй лабораторию внимательно - возможно, найдёшь какие-то пути, которые помогут в решении этой задачи.

Рекомендуемые утилиты: burp suite, dirsearch, ffuf и др.
Цель работы: исследование web-приложения и получение доступа к флагу.
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление корректного флага.

Web-2 - Зельеваренье (2/2)

В заброшенной лаборатории ты обнаружил варочную стойку с таинственным зельем. В колбе бурлит странная жидкость. Все твои зелья бесполезны, но если правильно изменить ингредиенты, можно создать могущественное 'Зелье администратора', которое откроет доступ к секретному пути /admin.

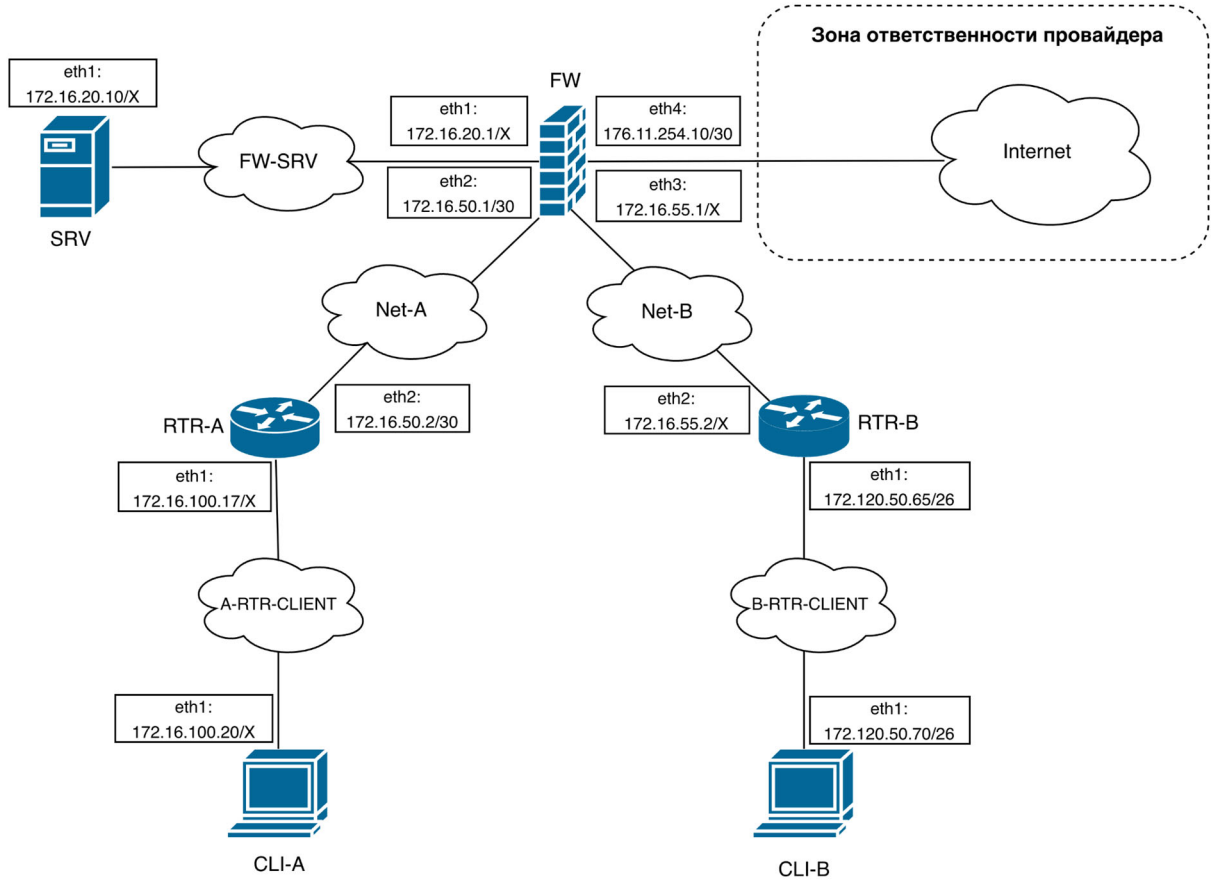
Рекомендуемые утилиты: burp suite, python и др.
Цель работы: получить способности админа и найти флаг в /admin

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 комбинация аргументов позволяет задать маршрут по-умолчанию на SRV для реализации доступа к глобальной сети? Введите в поле ответа номер варианта (число 1, 2, 3, 4 или 5).

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

Варианты ответа

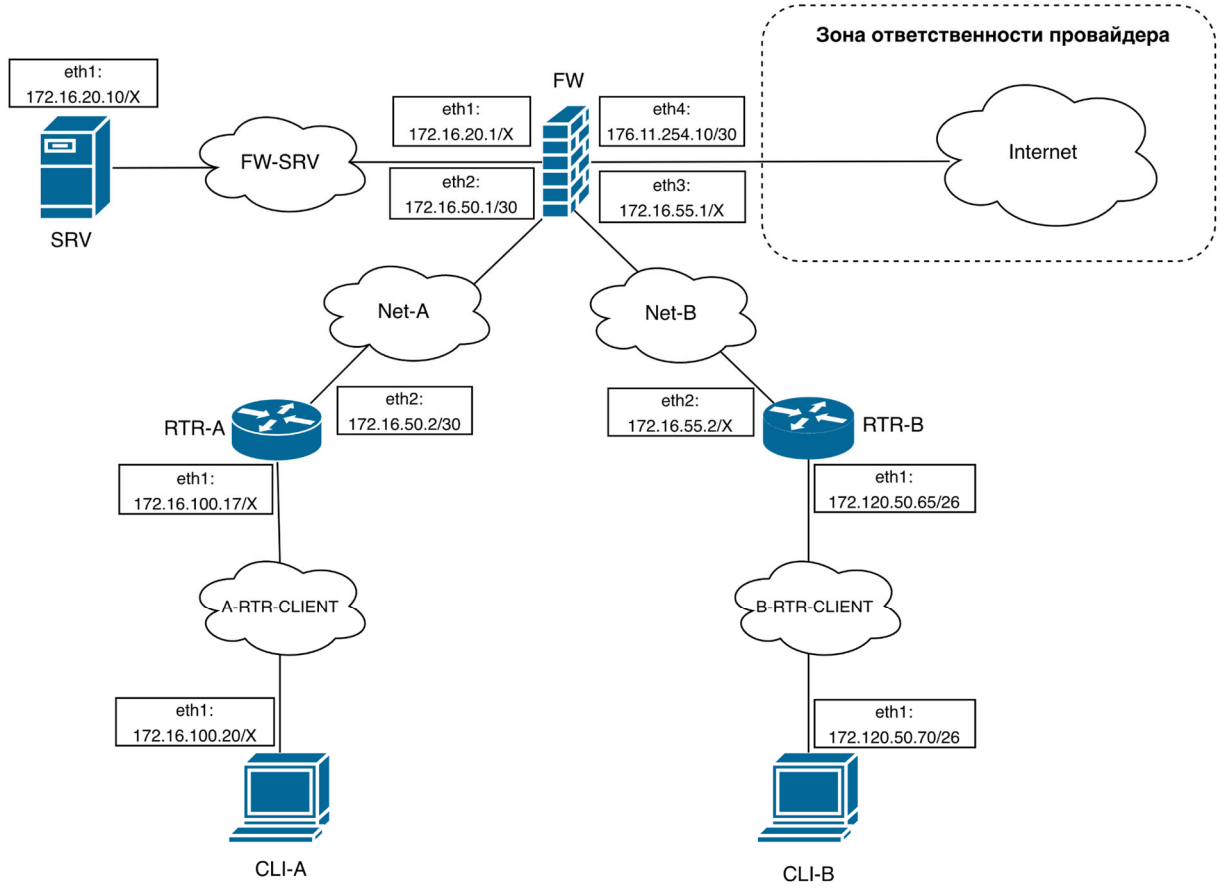
1. route add 0.0.0.0 mask 0.0.0.0 via eth1
2. route add 0.0.0.0 mask 0.0.0.0 via 176.11.254.10
3. route add default gw 172.16.20.1
4. route add default gw 176.11.254.10
5. route add default gw 176.11.254.10/33

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.



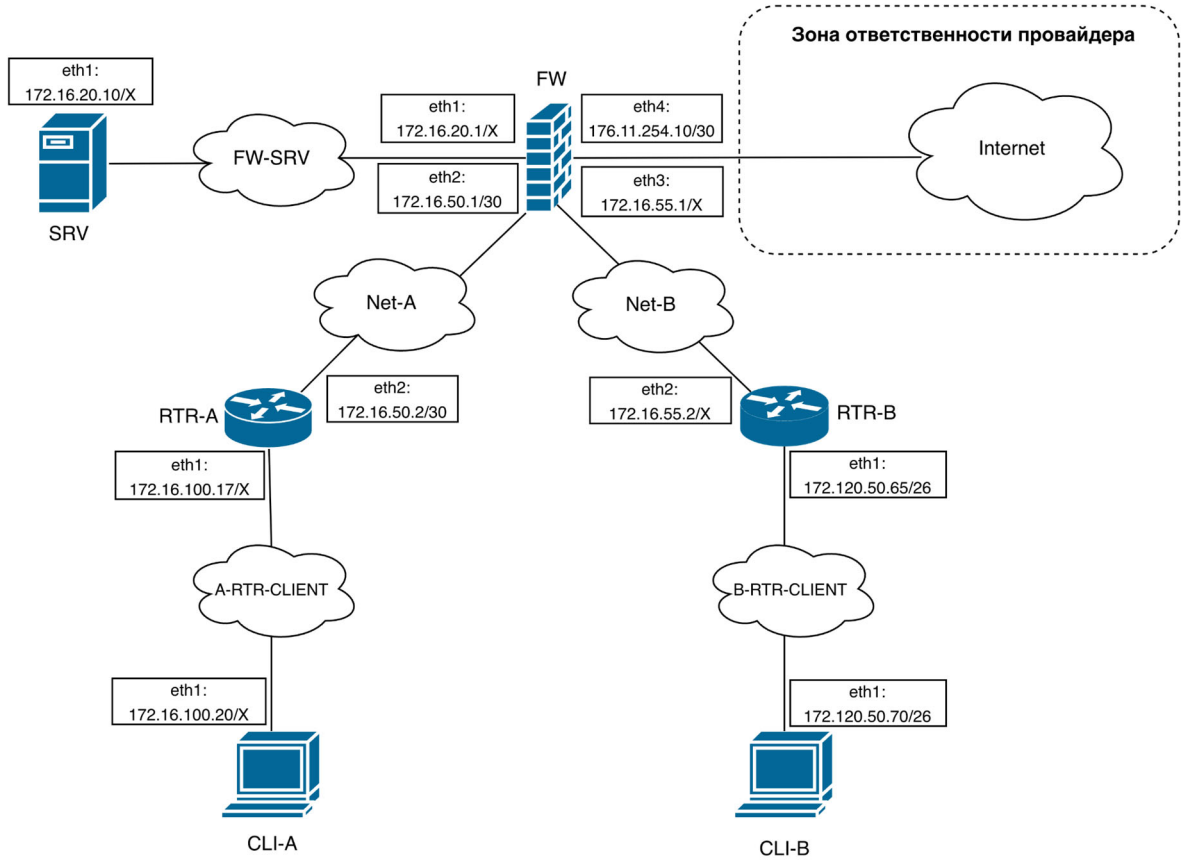
Какая максимальная длина префикса сети, которую можно задать для подсети FW-SRV, чтобы все её узлы оставались в одной подсети? Число попыток ввода: 2 раза

ВАЖНО: В ответ запишите только число (например, 24). 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.



SRV нужно настроить таким образом, чтобы весь HTTPS трафик автоматически перенаправлялся на прокси-сервер, который функционирует на 444 порту. Какая комбинация аргументов позволяет это выполнить?

iptables -t nat -A PREROUTING -p tcp ПАРАМЕТР1 ПАРАМЕТР2 -j ПАРАМЕТР3 --to-port 444

Выберите 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

Forensics 1 - Зараженный лаунчер Pinecraft (1/3)

Несколько игроков пожаловались, что после установки "улучшенного" лаунчера ZLauncher-Premium их аккаунты были взломаны. У Вас есть установочный файл и дамп процесса лаунчера. Найдите вредоносный код и определите, куда утекают данные.

Флаг **№1** необходимо сдать в формате: ***MD5 хеш вредоносного файла в лаунчере***. Ответ нужно сдавать без обертки.
Рекомендуемые утилиты: tar, unzip, jar, md5sum, strings, grep и др.
Цель работы: анализ вредоносного ПО, поиск индикаторов компрометации
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 1 - Зараженный лаунчер Pinecraft (2/3)

Несколько игроков пожаловались, что после установки "улучшенного" лаунчера ZLauncher-Premium их аккаунты были взломаны. У Вас есть установочный файл и дамп процесса лаунчера. Найдите вредоносный код и определите, куда утекают данные.

Флаг **№2** необходимо сдать в формате: ***URL, куда отправляются пароли игроков***. Ответ сдавать без обертки vsosh{}.

Ссылку на ресурс обязательно укажите с полным абсолютным путем (ответ принимается как с указанием протокола, так и без него).

Примеры: my-site.com/some/path, http://another-domain.com/home

Рекомендуемые утилиты: tar, unzip, jar, md5sum, strings, grep и др.
Цель работы: анализ вредоносного ПО, поиск индикаторов компрометации
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 1 - Зараженный лаунчер Pinecraft (3/3)

Несколько игроков пожаловались, что после установки "улучшенного" лаунчера ZLauncher-Premium их аккаунты были взломаны. У Вас есть установочный файл и дамп процесса лаунчера. Найдите вредоносный код и определите, куда утекают данные.

Флаг **№3** необходимо сдать в формате: ***Ключ для расшифровки логов лаунчера***. Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: tar, unzip, jar, md5sum, strings, grep и др.
Цель работы: анализ вредоносного ПО, поиск индикаторов компрометации
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 2 - Читерский клиент (1/3)

Игрок xX_ProGamer_Xx был забанен античитом за использование недопустимых модификаций. Он утверждает, что его аккаунт взломали. Администрация сделала дамп памяти его игрового клиента в момент обнаружения читов. Проанализируйте дамп и определите, какие именно читы использовались.

Флаг **№1** представляет собой **версию чит-клиента**. Ответ сдавать без обертки vsosh{}.

Рекомендуемые утилиты: strings, grep, xxd и др.
Цель работы: анализ дампа памяти, поиск следов чит-клиентов
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 2 - Читерский клиент (2/3)

Игрок xX_ProGamer_Xx был забанен античитом за использование недопустимых модификаций. Он утверждает, что его аккаунт взломали. Администрация сделала дамп памяти его игрового клиента в момент обнаружения читов. Проанализируйте дамп и определите, какие именно читы использовались.

Флаг **№2**: **ID активного в момент бана чит-модуля**. Ответ сдавать нужно без обертки.

Рекомендуемые утилиты: strings, grep, xxd и др.
Цель работы: анализ дампа памяти, поиск следов чит-клиентов
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 2 - Читерский клиент (3/3)

Игрок xX_ProGamer_Xx был забанен античитом за использование недопустимых модификаций. Он утверждает, что его аккаунт взломали. Администрация сделала дамп памяти его игрового клиента в момент обнаружения читов. Проанализируйте дамп и определите, какие именно читы использовались.

Флаг **№3**: **UUID-токен сессии игрока**. Ответ сдавать нужно без обертки.

Рекомендуемые утилиты: strings, grep, xxd и др.
Цель работы: анализ дампа памяти, поиск следов чит-клиентов
Итог работы: получить доступ к флагу.

Критерий оценки: предоставление правильного флага.

Reverse-1 – Забытый рецепт крафта (1/1)

В древних руинах ты обнаружил таинственный свиток с рецептом легендарного артефакта. Но кто-то разбросал ингредиенты рецепта по разным сундукам в соседних комнатах. Найди все компоненты и узнай секрет древнего крафта!

Рекомендуемые утилиты: bash, python и др.

Цель работы: Собрать разные компоненты кода и восстановить флаг.

Итог работы: получить полный флаг из предоставленного кода.

Критерий оценки: предоставление правильного флага.

Reverse-2 - Механизм из майнкрафта (1/2)

В заброшенной крепости ты нашел сундук, защищенный сложным редстоуновым механизмом, Механизм требует особого кода. Рядом с каждый рычагом стоят таблички с загадочными правилами и математическими формулами. Изучи схему редстоунов и найди правильный код, чтобы активировать механизм и открыть сундук с сокровищами!

Рекомендуемые утилиты: Ghidra, Python и др.

Цель работы: Подобрать правильную строку для прохождения четырех проверок

Итог работы: получить доступ к первому флагу.

Критерий оценки: предоставление правильного флага.

Reverse-2 - Механизм из майнкрафта (2/2)

В заброшенной крепости ты нашел сундук, защищенный сложным редстоуновым механизмом, Механизм требует особого кода. Рядом с каждый рычагом стоят таблички с загадочными правилами и математическими формулами. Изучи схему редстоунов и найди правильный код, чтобы активировать механизм и открыть сундук с сокровищами!

Рекомендуемые утилиты: Ghidra, Python и др.

Цель работы: Подобрать правильную строку для прохождения шести проверок

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 к 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 магазина от читера (1/1)

Дружище, читер получил доступ к чужим покупкам и ключам. Нужно починить форму просмотра заказа так, чтобы пользователи видели только свои заказы, а админы — могли смотреть все. Для этого мы тебе дадим онлайн-IDE, но учти, нужно писать код без ошибок.

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 приема соискателей 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 документ загрузил пользователь? Укажите название включая расширение.

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 приема соискателей 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.

На какой ip:port отработал reverse shell? Укажите ответ в формате ip:port.

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 приема соискателей 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 исполняемого файла злоумышленник повысил привилегии? Укажите полный путь до файла.

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 приема соискателей 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 нашел файл для повышения привилегий?

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 приема соискателей 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 предположительно получил хэши пользователей?

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 - Тайна заброшенной шахты (1/1)

Шахтер! В глубинах заброшенной алмазной шахты обнаружен древний сундук с загадочной табличкой. Нам известно лишь, что послание начиналось с 'vsosh{'. Помоги расшифровать руны и найти путь к сокровищам!

Рекомендуемые утилиты**:** python, sympy

Цель работы**:** Расшифровать сообщение и получить флаг

Итог работы: Расшифрованное сообщение

Критерий оценки**:** Предоставление правильного флага

Privesc-1 - Креатив (1/1)

Ты застрял в режиме выживания на сервере, но знаешь, что можешь переключиться в креатив, но сервер требует пароль администратора!

Рекомендуемые утилиты: ssh, bash

Цель работы: Повысить привилегии, чтобы получить доступ к флагу /root/flag.txt и прочитать его

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 книге, в которой 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 книге, в которой 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