Практическое задание для регионального этапа всероссийской олимпиады школьников по технологии 2025 – 2026 учебный год
Профиль “Информационная Безопасность”, 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. 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 проверить работоспособность ПК участника, доступность с виртуальной машины участника платформы ctfd, наличие инструкций.

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,

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

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.

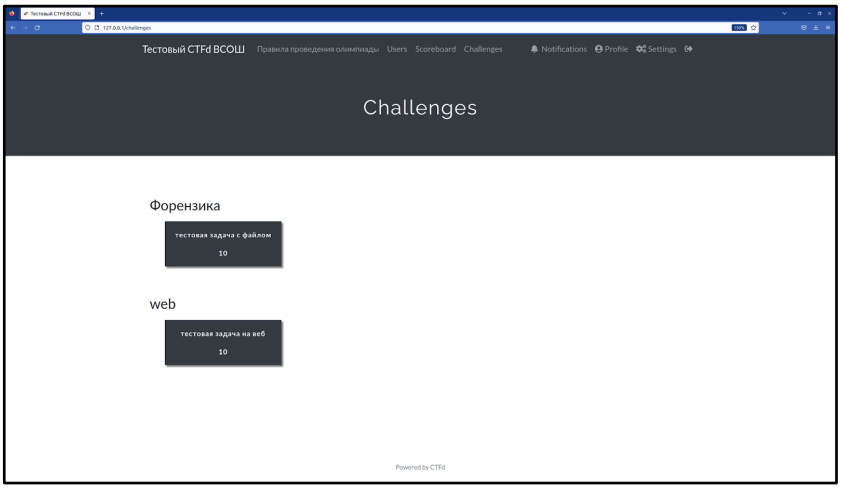


Рисунок 1 – примерный вид экранного интерфейса Платформы с заданиями

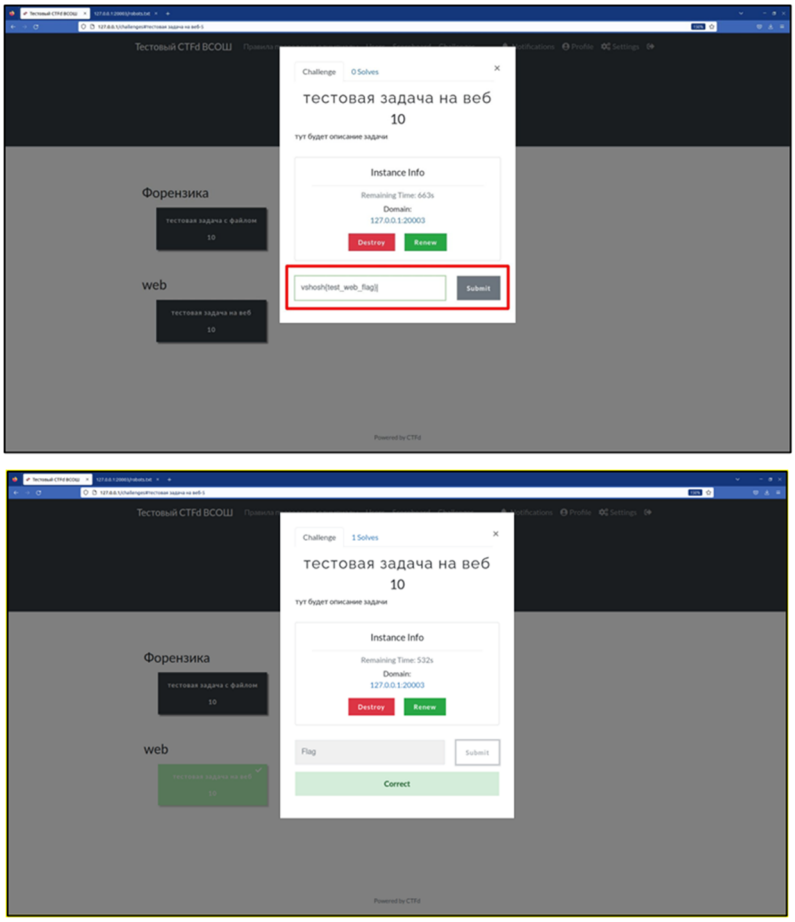


Рисунок 2 – пример успешного ввода флага. Задание засчитано.

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 11 классов

№ Задания	Тематика задания	Критерии оценки	Кол-во баллов
1.	**Crypto-1**	Факт размещения участником в поле для ввода 1 корректного флага	1
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 7 корректных флагов	1+1+1+1+1+1+1 =7
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	4
14.	**Misc-1**	Факт размещения участником в поля для ввода 2 корректных флагов	1+3
Σ			**70**

Задания 11 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!

СЗИ-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..56 -K ...и дальше неразборчиво. Ключ он не знал. Попробуем перебрать по словарю и получить координаты бастиона!

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

Web 1 - Дальние земли (1/2)

Ты нашёл портал, который перемещает на дальние острова Энда. В этих землях разбросано множество шалкеров - говорят, их около тысячи! А один из этих шалкеров содержит древнюю книгу с флагом.

Рекомендуемые утилиты: burp suite, python и др.
Цель работы: Найти и скачать изображение с флагом
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление корректного флага.

Web 1 - Дальние земли (2/2)

Оказывается, ты нашел не обычный портал в Энд. Он работает как прокси, но его защита настроена странно! При определенных условиях он позволяет заглянуть в далекие земли. А где-то там есть сундук с приватными изображениями флага, недоступный через обычный портал.

Рекомендуемые утилиты: burp suite, python и др.
Цель работы: Использовать портал-прокси для телепортации в запретную зону и прочитать флаг с картинки
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление корректного флага.

Web 2 - Библиотека Крепости (1/2)

В подземельях крепости ты находишь древнюю библиотеку. На табличке рядом с кафедрой записки хранителя: «Все печати принимаются» — будто бы любой токен сойдёт, лишь бы в нём была правильная запись.

Рекомендуемые утилиты: burp suite, curl и др.
Цель работы: Получить флаг, подменив подпись и задекларировав права администратора
Итог работы: получить доступ к флагу.

Критерий оценки: предоставление корректного флага.

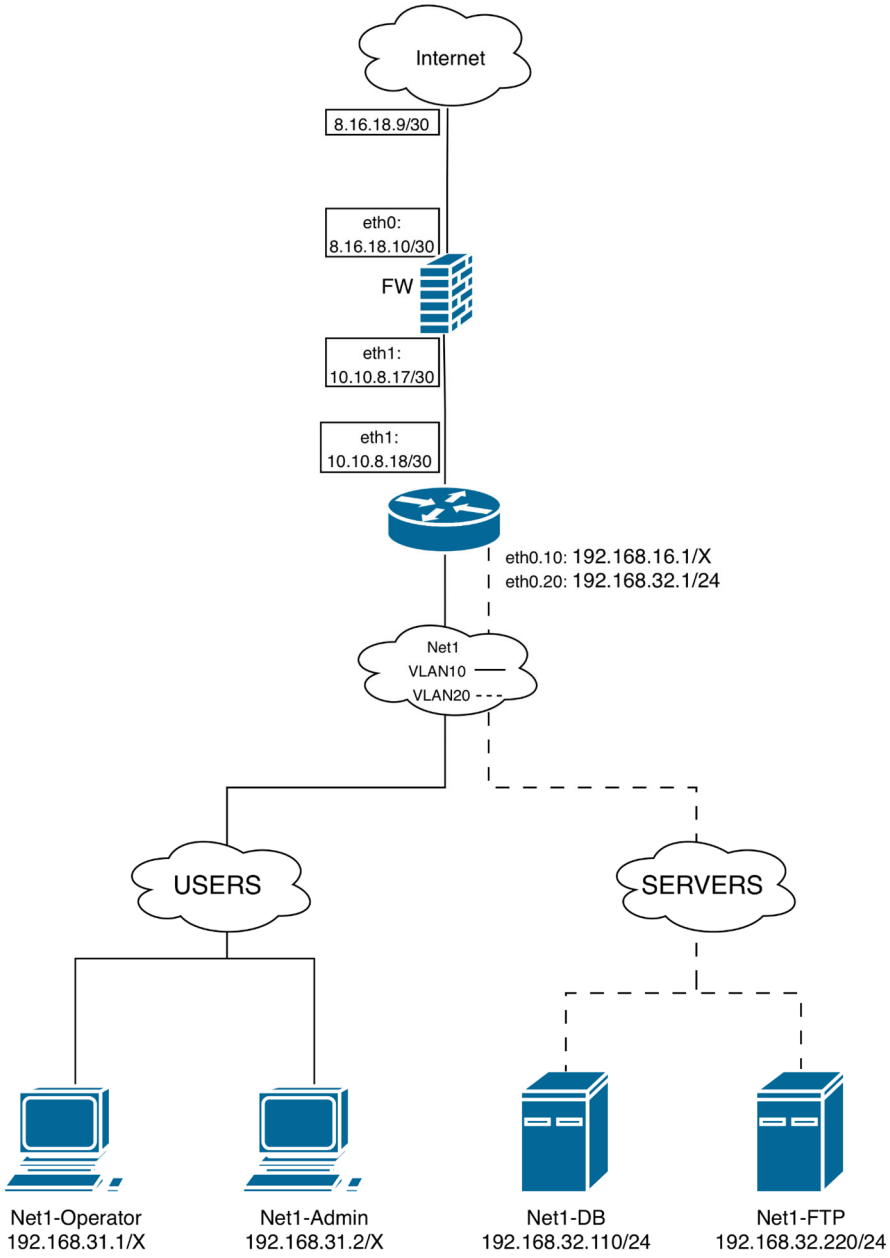
Web 2 - Библиотека Крепости (2/2)

Под крепостью обнаружился скрытый переход в зал с наковальнями и стойками для брони. На табличках выгравировано: «RS256, HS256, ES256». Похоже, сюда пускают только тех, кто приносит особые ключи и показывает их на входе.

Рекомендуемые утилиты: burp suite, curl, python, openssl и др.
Цель работы: Получить флаг, подменив подпись и задекларировав права администратора
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.



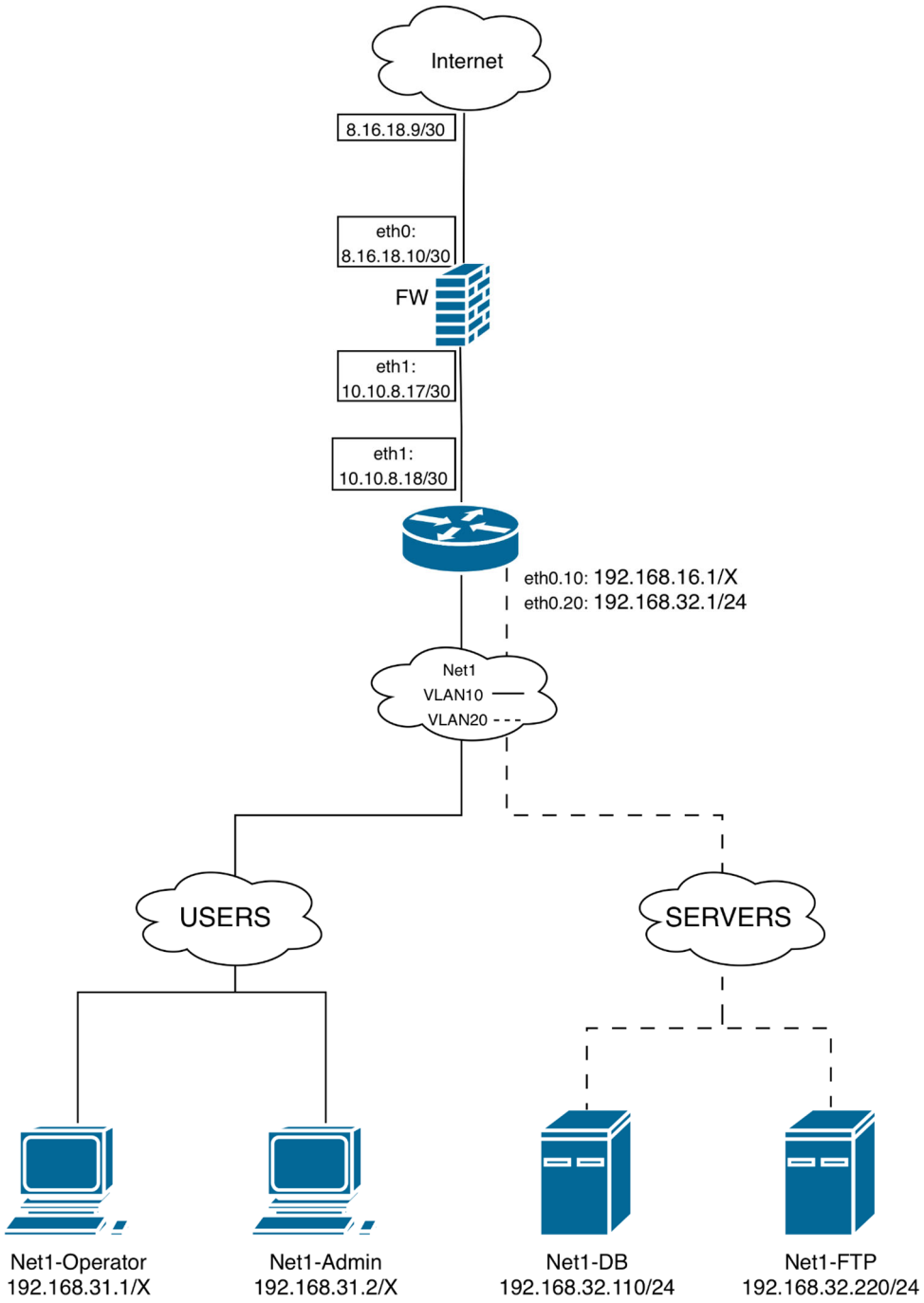
Какая максимальная длина префикса сети, которую можно задать для подсети USERS (VLAN10) чтобы все её узлы оставались в одной подсети? В ответ запишите только число (например, 24).

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 в поле ввода флага

Network -1 – сети (2/3)

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



Какое правило iptables нужно добавить на FW для SNAT/MASQUERADE трафика из внутренних VLAN в Интернет?

iptables -t <ПАРАМЕТР1> -A <ПАРАМЕТР2> -s 192.168.0.0/16 -o <ПАРАМЕТР3> -j MASQUERADE

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

ПАРАМЕТР1_ПАРАМЕТР2_ПАРАМЕТР3

Например:

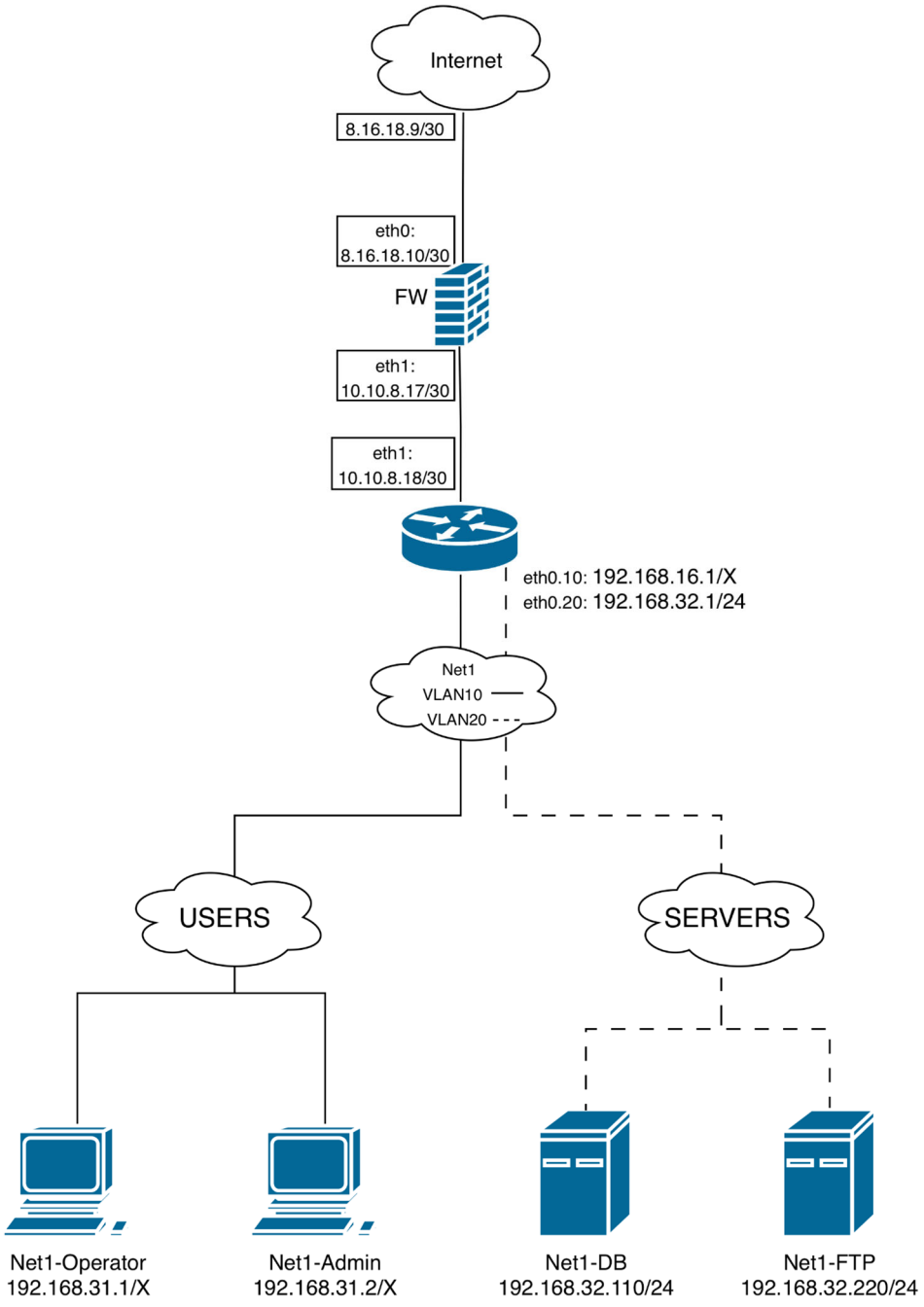
Если ПАРАМЕТР1 = SEND, ПАРАМЕТР2 = ++tuda, ПАРАМЕТР3 = 2026 то итоговый флаг будет SEND_++tuda_2026

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. На основе этой схемы ответьте на вопросы.



Какой адрес сети используется на линке между FW и маршрутизатором?

1. 10.10.8.16
2. 10.10.8.17
3. 10.10.8.18
4. 10.10.8.19
5. 10.10.0.0

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 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

Forensics 1 - Криптомайнер в контейнерах (1/3)

На хостинге Pinecraft серверов обнаружена подозрительная активность. Кто-то запускает криптомайнеры в Docker контейнерах вместо игровых серверов.

Администратор платформы успел сделать экспорт подозрительных Docker образов и собрать логи системы, упаковав всё в защищённый архив. Однако после этого он перестал выходить на связь — возможно, злоумышленники обнаружили его действия. К счастью, администратор использовал один из своих типичных паролей. По данным из предыдущих утечек, он предпочитает простые словарные пароли.

Ваша задача: получить доступ к архиву с уликами, найти вредоносные контейнеры и определить масштаб проблемы.

Флаг **№1** необходимо сдать в формате: ***SHA256-хеш вредоносного Docker образа, содержащего образец майнера xmrig (первые 12 символов)***. Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: tar, grep, strings, awk, sed и др.
Цель работы: анализ контейнеризированных угроз
Итог работы: получить доступ к флагу
Критерий оценки: предоставление правильного флага.

Forensics 1 - Криптомайнер в контейнерах (2/3)

На хостинге Pinecraft серверов обнаружена подозрительная активность. Кто-то запускает криптомайнеры в Docker контейнерах вместо игровых серверов.

Администратор платформы успел сделать экспорт подозрительных Docker образов и собрать логи системы, упаковав всё в защищённый архив. Однако после этого он перестал выходить на связь — возможно, злоумышленники обнаружили его действия. К счастью, администратор использовал один из своих типичных паролей. По данным из предыдущих утечек, он предпочитает простые словарные пароли.

Ваша задача: получить доступ к архиву с уликами, найти вредоносные контейнеры и определить масштаб проблемы.

Флаг **№2** необходимо сдать в формате: ***Адрес криптокошелька для майнинга***. Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: tar, grep, strings, awk, sed и др.
Цель работы: анализ контейнеризированных угроз
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 1 - Криптомайнер в контейнерах (3/3)

На хостинге Pinecraft серверов обнаружена подозрительная активность. Кто-то запускает криптомайнеры в Docker контейнерах вместо игровых серверов.

Администратор платформы успел сделать экспорт подозрительных Docker образов и собрать логи системы, упаковав всё в защищённый архив. Однако после этого он перестал выходить на связь — возможно, злоумышленники обнаружили его действия. К счастью, администратор использовал один из своих типичных паролей. По данным из предыдущих утечек, он предпочитает простые словарные пароли.

Ваша задача: получить доступ к архиву с уликами, найти вредоносные контейнеры и определить масштаб проблемы.

Флаг **№3** необходимо сдать в формате: ***Шестнадцатеричная запись ЧИСЛА ПРОЦЕНТОВ суммарного CPU usage всех майнеров***.

Подразумевается сумма процентов без нормировки. Если получившийся результат - не целое число, тогда округлите его до ближайшего целого (по правилам округления). Пример: 2196.5 (%) → 2197. Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: tar, grep, strings, awk, sed и др.
Цель работы: анализ угроз контейнеризации
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 2 - Свиноплагин (1/3)

Плагин EconomyPlus, установленный на тысячах серверов, оказался заражён. Вредоносный код маскируется под легитимную логику, но на самом деле превращает сервер в зомбированного агента — «свинозомби», который шлёт данные на C&C (command & control server).
У вас есть копия JAR-файла и дамп трафика с заражённого сервера. Найдите следы заражения.

Флаг **№1** необходимо сдать в формате: ***Порт управляющего сервера (C&C-server)***. Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: unzip, strings, grep, base64 и др.
Цель работы: анализ JAR файла, поиск вредоносного кода, выявление вредоносного поведения
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 2 - Свиноплагин (2/3)

Плагин EconomyPlus, установленный на тысячах серверов, оказался заражён. Вредоносный код маскируется под легитимную логику, но на самом деле превращает сервер в зомбированного агента — «свинозомби», который шлёт данные на C&C (command & control server).
У вас есть копия JAR-файла и дамп трафика с заражённого сервера. Найдите следы заражения.

Флаг **№2** необходимо сдать в формате: ***Название функции в коде, которая крадет данные***. Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: unzip, strings, grep, base64 и др.
Цель работы: анализ JAR файла, поиск вредоносного кода, выявление вредоносного поведения
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Forensics 2 - Свиноплагин (3/3)

Плагин EconomyPlus, установленный на тысячах серверов, оказался заражён. Вредоносный код маскируется под легитимную логику, но на самом деле превращает сервер в зомбированного агента — «свинозомби», который шлёт данные на C&C (command & control server).
У вас есть копия JAR-файла и дамп трафика с заражённого сервера. Найдите следы заражения.

Флаг **№3** необходимо сдать в формате: ***Пароль администратора, который утек к злоумышленникам***. Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: unzip, strings, grep, base64 и др.
Цель работы: анализ JAR файла, поиск вредоносного кода, выявление вредоносного поведения

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

Reverse 1 – Тайна эндермена (1/1) -

В крепости Края ты нашел книгу, которую писал эндермен. Но эндермен постоянно телепортировался во время написания, поэтому книга полна хаотичных записей и повторений! Среди всего этого беспорядка спрятано истинное заклинание, которое закодировано особыми эндер-рунами. Найди его среди хаоса и расшифруй послание из Края!

Рекомендуемые утилиты: bash, Ghidra, Python и др.
Цель работы: Очистить код от хаоса, чтобы найти флаг
Итог работы: получить доступ к флагу.
Критерий оценки: предоставление правильного флага.

Reverse 2 - Продвинутый майнкрафтер (1/2)

В секретной лаборатории был найден древний терминал с двухфакторной аутентификацией но никто не понимает почему он не включается. Твоя задача — заставить его работать.

Рекомендуемые утилиты: Ghidra, Python и др.

Цель работы: Найти XOR ключ в памяти программы (можно извлечь в дебагере)
Итог работы: Получить доступ к первому флагу
Критерий оценки: предоставление правильного флага.

Reverse 2 - Командный блок (2/2)

В секретной лаборатории был найден древний терминал с двухфакторной аутентификацией но никто не понимает почему он не включается. Твоя задача — заставить его работать.

Рекомендуемые утилиты: Ghidra, Python и др.
Цель работы: Получить финальный флаг, изменив результат проверки
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 2 - Защити лаунчер от хакеров (1/1)

Хакеры взломали редирект после входа в лаунчер Minecraft. Почини функцию редиректа так, чтобы хакеры не могли украсть аккаунты игроков.

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 3 - Деревенский сыщик (1/7)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но сервис хранения рецептов зелий оказался захвачен и разорен. 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 был загружен на хост? 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 все вопросы
Критерии оценки: предоставление правильных ответов

СЗИ 3 - Деревенский сыщик (2/7)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но сервис хранения рецептов зелий оказался захвачен и разорен. 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 файл логов содержал учетные данные? Укажите название файла 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 все вопросы

Критерии оценки: предоставление правильных ответов

СЗИ 3 - Деревенский сыщик (3/7)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но сервис хранения рецептов зелий оказался захвачен и разорен. 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 протокол использовал злоумышленник для подключения к хосту 2? Укажите протокол в верхнем регистре.

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 все вопросы

Критерии оценки: предоставление правильных ответов

СЗИ 3 - Деревенский сыщик (4/7)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но сервис хранения рецептов зелий оказался захвачен и разорен. 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 скрипт использовался для разведки на хосте 2? Укажите название файла 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 все вопросы

Критерии оценки: предоставление правильных ответов

СЗИ 3 - Деревенский сыщик (5/7)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но сервис хранения рецептов зелий оказался захвачен и разорен. 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.

Какая папка использовалась для повышения привилегий на хосте 2? Укажите полный путь.

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 все вопросы

Критерии оценки: предоставление правильных ответов

СЗИ 3 - Деревенский сыщик (6/7)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но сервис хранения рецептов зелий оказался захвачен и разорен. 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.

Какую учетную запись использовал злоумышленник для подключения к базе данных?

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 все вопросы

Критерии оценки: предоставление правильных ответов

СЗИ 3 - Деревенский сыщик (7/7)

Совсем не давно на деревню жителей произошло нападение. Главные службы не пострадали, но сервис хранения рецептов зелий оказался захвачен и разорен. 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.

Откуда были выгружены данные пользователей? Напишите название базы данных и таблицы в формате: db_name:table_name

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 все вопросы

Критерии оценки: предоставление правильных ответов

Crypto 1 - Секрет командного блока

Исследуя морской данж, ты находишь странный командный блок, светящийся красным светом. Рядом стоит табличка:

"Я создал этот командный блок для защиты своих самых ценных ресурсов, использовав криптографический алгоритм RSA..."

На дисплее командного блока отображаются три числа:

- n (какое-то большое число)

- e (публичный ключ)

- c (зашифрованная команда)

Сможешь ли ты найти уязвимость в этой защите и активировать командный блок?

Рекомендуемые утилиты: python, sympy

Цель работы: Расшифровать сообщение и получить флаг

Итог работы: Расшифрованное сообщение

Критерий оценки: Предоставление правильного флага

Privesc 1 - Портал пиглинов (1/1)

В подземном царстве Нижнего мира пиглины построили специальный портал, который работает через древний сокет. Используй этот портал пиглинов, чтобы добраться до их сокровищ!

Рекомендуемые утилиты: ssh, bash, python, socat

Цель работы: Использовать мисконфигурацию сервера, повысить привилегии 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 целой библиотеке, и в одной из книг 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 целой библиотеке, и в одной из книг 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