Задания 9 КЛАСС

Crypto-1 - Страж сертификатов безопасности (1/1) - 1 балл

Архивариус из энда прислал загадочный свиток и подсказки для разгадки его содержимого. Вспомни чему тебя учили прошлые испытания и расшифруй свиток.

Рекомендуемые утилиты: openssl, bash, python

Цель работы: Получить флаг

Критерий оценки: Предоставление правильного флага

Crypto-2 - Древний страж (1/1) - 6 баллов

Древний страж данжа принимает целое x и возвращает (flag * x) mod p, где p - неизвестное простое 64-битное число. Запрещено использовать x = 0 или x = 1.

Формат флага: число - целое значение.

Рекомендуемые утилиты: netcat, python

Цель работы: Восстановить флаг через запросы к стражу

Критерий оценки: Предоставление правильного флага

Web-1 - Древний город (1/2) - 1 балл

В тёмных глубинах ты находишь вход в древний город. На стене у портала висят потрёпанные таблички — кто-то пытался спрятать путь, оставив подсказки для роботов и внимательных исследователей.

Рекомендуемые утилиты: burp suite, curl

Цель работы: Найти скрытый путь и получить флаг

Критерий оценки: Предоставление правильного флага

Web-1 - Древний город (2/2) - 3 балла

В архивной книге ты замечаешь запись: «Если увидишь табличку admin у портала, знай — он часто возвращается сюда». Похоже, мастера, ставившие блоки доступа, оставили лишние рычаги в механизмах — достаточно знать, какой рычаг переключить.

Рекомендуемые утилиты: burp suite, curl

Цель работы: Получить доступ к тайному залу и найти флаг в /secret-hall

Критерий оценки: Предоставление правильного флага

Web-2 - Магазин лицензий (1/2) - 2 балла

Мы запустили новый магазин лицензий майнкрафт с микросервисной очередью RabbitMQ. Оплаты попадают в очередь, JSON и XML воркеры раздают лицензии асинхронно на почты.

Рекомендуемые утилиты: curl, dirsearch, ffuf

Цель работы: получить флаг

Критерий оценки: предоставление правильного флага

Web-2 - Магазин лицензий (2/2) - 4 балла

Мы запустили новый магазин лицензий майнкрафт с микросервисной очередью RabbitMQ. Оплаты попадают в очередь, JSON и XML воркеры раздают лицензии асинхронно. Попробуй купить самую крутую лицензию с плащом!

Рекомендуемые утилиты: curl, burp suite, python

Цель работы: получить флаг

Критерий оценки: предоставление правильного флага

Network-1 - Сеть деревни Minecraft (1/3) - 1 балл

На карте мира Minecraft показана сеть деревни: компьютеры Стива, Алекс, Херобрина и Эндермена подключены к коммутатору (как к редстоун-раздатчику), а дальше трафик уходит через роутеры R1 и R2 в Интернет-портал. Отдельно за роутером R3 расположена «серверная шахта» с SRV1 и SRV2. Используя эту схему, ответьте на вопрос ниже.

Что нужно найти: минимальную по размеру подсеть (или с максимальным префиксом сети), чтобы все 4 ПК гарантированно оказались в одной сети. Ответ укажите в формате /20.

Рекомендуемые утилиты: текстовый редактор, черновик для вычислений

Цель работы: определить корректный префикс подсети по условию задания

Итог работы: корректно вписать ответ

Критерий оценки: предоставление корректного ответа

Network-1 - Сеть деревни Minecraft (2/3) - 2 балла

В деревне два выхода в Интернет — через R1 и через R2. Алекс на своем ПК (192.168.10.32) «настроила все сразу», поэтому в системе несколько маршрутов по умолчанию.

На устройствах получены листинги, представленные в книге Listings.txt. Выберите все верные утверждения из книги Statements.txt.

Что нужно найти: номера всех верных утверждений. Ответ запишите через подчеркивание в порядке возрастания, например: 1_3_5

Рекомендуемые утилиты: текстовый редактор, черновик для анализа маршрутизации

Цель работы: проанализировать выбор маршрута по таблице ip route, metric и базовым правилам Linux routing

Итог работы: корректно вписать ответ

Критерий оценки: предоставление корректного ответа

Network-1 - Сеть деревни Minecraft (3/3) - 1 балл

В редстоун-переключателе поднят роутер Адская Стена, через который проходят редстоун-трафик между сетью деревни 192.168.10.0/24 и серверной сетью 192.168.20.0/24. На стороне серверной сети находится командный блок SRV1 (192.168.20.10) с Minecraft-сервисом на 25565/tcp, а также дополнительные сервисы и узлы, доступ к которым открывать нельзя.

Войди переключатель по SSH и настрой его iptables так, чтобы: - жители из сети деревни могли подключаться к SRV1 только по 25565/tcp - остальной новый трафик из 192.168.10.0/24 в серверную сеть оставался запрещенным

В стенде уже настроена базовая политика защиты: FORWARD DROP, а также разрешен ESTABLISHED,RELATED.

Рекомендуемые утилиты: ssh, bash, iptables

Цель работы: настроить корректное правило фильтрации iptables

Итог работы: получить строку ответа от чекера

Критерий оценки: предоставление корректного флага

Forensics-1 - Подозрительная скупка на Гранд-Турнире (1/2) - 1 балл

Финал Гранд-Турнира Pinecraft был в самом разгаре: лучшие игроки сражались за Кубок Алмазного Меча. Но в разгар матча что-то пошло не так — магазин зелий начал продавать алмазную броню за 1 изумруд, а на сервере появились файлы, которых там быть не должно.

Админ Стив успел запустить перехват трафика прежде чем выдернуть кабель. Теперь дамп у тебя. Разберись, кто устроил этот хаос.

Что нужно найти: имя учётной записи, под которой атакующий авторизовался в веб-магазине

Рекомендуемые утилиты: Wireshark, tshark

Цель работы: анализ сетевого трафика, поиск HTTP-запросов атакующего

Критерий оценки: предоставление корректного флага

Forensics-1 - Подозрительная скупка на Гранд-Турнире (2/2) - 1 балл

Финал Гранд-Турнира Pinecraft был в самом разгаре: лучшие игроки сражались за Кубок Алмазного Меча. Но в разгар матча что-то пошло не так — магазин зелий начал продавать алмазную броню за 1 изумруд, а на сервере появились файлы, которых там быть не должно.

Админ Стив успел запустить перехват трафика прежде чем выдернуть кабель. Разберись, что именно атакующий загрузил на сервер.

Что нужно найти: название файла, который атакующий загрузил через панель администратора

Рекомендуемые утилиты: Wireshark, tshark

Цель работы: анализ сетевого трафика, исследование HTTP-запросов

Критерий оценки: предоставление корректного флага - название файла с расширением

Forensics-2 - Образ диска взломанного сервера Pinecraft (1/2) - 1 балл

После инцидента со взломом магазина зелий администратор Стив экстренно остановил сервер Pinecraft и снял образ диска. На диске остались логи сервера и следы деятельности атакующего.

Смонтируй образ диска, изучи файловую систему и найди в логах IP-адрес, с которого действовал злоумышленник.

Что нужно найти: IP-адрес, с которого атакующий получил несанкционированный доступ к серверу

Рекомендуемые утилиты: mount, grep, less, cat

Цель работы: монтирование образа диска, анализ лог-файлов сервера

Критерий оценки: предоставление корректного флага

Forensics-2 - Образ диска взломанного сервера Pinecraft (2/2) - 2 балла

Изучая файловую систему, ты обнаружишь директорию /minecraft/backups/ — но она окажется подозрительно пустой. Администратор Стив точно помнит, что хранил там файл admin_backup.txt с важным секретным паролем. Похоже, атакующий удалил его, пытаясь замести следы.

Но удаление файла в Linux — не то же самое, что его уничтожение. На файловой системе ext4 содержимое удалённого файла часто остаётся на диске до тех пор, пока его место не будет перезаписано новыми данными.

Что нужно найти: секретный пароль из удалённого файла admin_backup.txt

Рекомендуемые утилиты: strings, grep

Цель работы: восстановление удалённых данных с образа диска ext4

Критерий оценки: предоставление корректного флага

Forensics-3 - Неизвестное зачарование (1/2) - 2 балла

Мистическое зло проникло в наши архивы - оно требует изумрудов. Мы вынуждены откупиться и отправить биткоин-изумруды на адрес. Но мы не можем понять,что за ID требует это зло. Одно понятно, расшифровывать нам не ничего не нужно - бизнес-процессы жителей важнее.

Найдите идентификатор процесса текстовика, в котором открыт спасительный файл. Пришлите его без обертки.

Рекомендуемые утилиты: volatility, strings, grep

Цель работы: Обнаружение идентификатора процесса

Критерий оценки: предоставление корректного флага

Forensics-3 - Неизвестное зачарование (2/2) - 3 балла

Мистическое зло проникло в наши архивы - оно требует изумрудов. Мы вынуждены откупиться и отправить биткоин-изумруды на адрес. Но мы не можем понять,что за ID требует это зло. Одно понятно, расшифровывать нам не ничего не нужно - бизнес-процессы жителей важнее.

Пришлите ID который был присвоен этому компьютеру атакующим без обертки.

Рекомендуемые утилиты: volatility, strings, grep

Цель работы: Обнаружение идентификатора

Критерий оценки: предоставление корректного флага-ID

Reverse-1 - Далекая вершина (1/1) - 3 балла

На вершине горы Эльбрус стоит 0x20 дом, в нем ты нашел странные книжки, но лишь одну из них ты можешь прочитать. Разберись с этими книжками чтобы найти флаг.

Рекомендуемые утилиты: grep, strings, cat, file

Цель работы: анализ ассемблерного листинга экзотической архитектуры

Критерий оценки: предоставление корректного флага

Reverse-2 - Двойной редстоуновый замок (1/2) - 3 балла

"Два флага. Два условия. Механизм честен: он скажет тебе всё, что нужно знать. Вопрос в том, поймёшь ли ты его."

Рекомендуемые утилиты: Ghidra, Python, pwntools

Цель работы: Изучить алгоритм проверки первого этапа и найти код, дающий первый флаг

Критерий оценки: Предоставление правильного флага

Reverse-2 - Двойной редстоуновый замок (2/2) - 3 балла

"Два флага. Два условия. Механизм честен: он скажет тебе всё, что нужно знать. Вопрос в том, поймёшь ли ты его."

Рекомендуемые утилиты: Ghidra, Python, pwntools

Цель работы: Изучить алгоритм проверки второго этапа и найти код, дающий второй флаг

Критерий оценки: Предоставление правильного флага

Pwn-1 - Single Block (1/1) - 8 баллов

В Нижнем Мире нашли терминал, умеющий шифровать ровно один блок. Вопрос в том, что он считает блоком.

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

Цель работы: Поиск и эксплуатация уязвимости в бинарном приложении

Критерий оценки: Получение корректного флага

Privesc-1 - Шахта двух игроков (1/2) - 2 балла

Ты заходишь в мир как steve. В его базе полно сундуков с мусором, табличками и люками. Где-то среди этих заметок спрятана подсказка, как зайти за второго игрока.

Рекомендуемые утилиты: ssh, bash

Цель работы: Найти учетные данные и получить первый флаг

Критерий оценки: Предоставление правильного флага

Privesc-1 - Шахта двух игроков (2/2) - 3 балла

Теперь ты играешь за alex. Разберись, как воспользоваться скрытыми редстоун-механизмами на сервере, чтобы получить второй флаг в /root/flag2.txt.

Рекомендуемые утилиты: ssh, bash

Цель работы: Получить второй флаг

Критерий оценки: Предоставление правильного флага

Misc-1 - Общее хранилище деревни (1/1) - 3 балла

В деревне есть общее хранилище. В нем лежит «замок», который оставил другой житель: ты можешь класть в хранилище свои вещи и даже редактировать замок. Нужно удалить замок и запустить программу: она откроет сокровищницу и выведет флаг.

Рекомендуемые утилиты: ssh, bash, rm

Цель работы: Удалить замок и выполнить файл для получения флага.

Критерий оценки: Предоставление правильного флага

СЗИ-1 - Деревенская подработка (1/1) - 3 балла

Поздравляем, тебя приняли в деревню торговцев главным защитником! Правда кажется, что в кибер-деревне сломался регулировщик запросов. Беги закрывать главные бреши в стене кода веб-сайта!

Рекомендуемые утилиты: ssh, python

Цель работы: изменение кода приложения.

Итог работы: получить флаг после верного исправления кода.

Критерий оценки: предоставление правильного флага.

СЗИ-2 - Сетевой голем (1/1) - 3 балла

Деревня рекрутеров все еще под атакой, кажется произошел пробив других веб-входов, а сетевой голем-защитник сломался и смог лишь записать логи атак. Нужно срочно починить правила работы сетевого голема и заблокировать все атаки, не навредив легитимным жителям деревни.

Рекомендуемые утилиты: веб-ide

Цель работы: написание правил для блокировки вредоносного трафика

Итог работы: получить флаг в проверяющей системе

СЗИ-3 - Хронология событий (1/8) - 1 балл

Кажется сетевые атаки прекратились, но внутри деревни эйчаров заметили свинозомби! Надо выяснить что случилось, составив подробный ход событий атаки и ответить на вопросы CEO-старосты. Но не забывай, староста занятой, у тебя есть лишь несколько попыток для каждого ответа!

Вопрос от старосты: Укажите какой утилитой перебирались директории на roundcube? Ответ в формате: название_утилиты.

ВАЖНО: Задание разбито на несколько отдельных вопросов, для ответа используется общий набор файлов логов. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют ограниченное число неудачных попыток - по 2 попытки ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, VS-code, текстовый редактор и др.

Цель работы: Прочитать логи и найти ответ на вопрос

Критерий оценки: Предоставление правильного ответа

СЗИ-3 - Хронология событий (2/8) - 1 балл

Кажется сетевые атаки прекратились, но внутри деревни эйчаров заметили свинозомби! Надо выяснить что случилось, составив подробный ход событий атаки и ответить на вопросы CEO-старосты. Но не забывай, староста занятой, у тебя есть лишь несколько попыток для каждого ответа!

Вопрос от старосты: Укажите какую уязвимость использовал злоумышленник для выполнения RCE. Ответ в формате: CVE-xxxx-xxxx.

ВАЖНО: Задание разбито на несколько отдельных вопросов, для ответа используется общий набор файлов логов. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют ограниченное число неудачных попыток - по 2 попытки ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, VS-code, текстовый редактор и др.

Цель работы: Прочитать логи и найти ответ на вопрос

Критерий оценки: Предоставление правильного ответа

СЗИ-3 - Хронология событий (3/8) - 1 балл

Кажется сетевые атаки прекратились, но внутри деревни эйчаров заметили свинозомби! Надо выяснить что случилось, составив подробный ход событий атаки и ответить на вопросы CEO-старосты. Но не забывай, староста занятой, у тебя есть лишь несколько попыток для каждого ответа!

Вопрос от старосты: Укажите какие скрипты для разведки злоумышленник загрузил на roundcube. Ответ в формате: скрипт1_скрипт2.

ВАЖНО: Задание разбито на несколько отдельных вопросов, для ответа используется общий набор файлов логов. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют ограниченное число неудачных попыток - по 2 попытки ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, VS-code, текстовый редактор и др.

Цель работы: Прочитать логи и найти ответ на вопрос

Критерий оценки: Предоставление правильного ответа

СЗИ-3 - Хронология событий (4/8) - 1 балл

Кажется сетевые атаки прекратились, но внутри деревни эйчаров заметили свинозомби! Надо выяснить что случилось, составив подробный ход событий атаки и ответить на вопросы CEO-старосты. Но не забывай, староста занятой, у тебя есть лишь несколько попыток для каждого ответа!

Вопрос от старосты: Какой командой злоумышленник повысил привилегии, включая путь до исполняемого файла и ключ?

ВАЖНО: Задание разбито на несколько отдельных вопросов, для ответа используется общий набор файлов логов. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют ограниченное число неудачных попыток - по 2 попытки ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, VS-code, текстовый редактор и др.

Цель работы: Прочитать логи и найти ответ на вопрос

Критерий оценки: Предоставление правильного ответа

СЗИ-3 - Хронология событий (5/8) - 1 балл

Кажется сетевые атаки прекратились, но внутри деревни эйчаров заметили свинозомби! Надо выяснить что случилось, составив подробный ход событий атаки и ответить на вопросы CEO-старосты. Но не забывай, староста занятой, у тебя есть лишь несколько попыток для каждого ответа!

Вопрос от старосты: Какой утилитой злоумышленник пробросил порты? Укажите название утилиты.

ВАЖНО: Задание разбито на несколько отдельных вопросов, для ответа используется общий набор файлов логов. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют ограниченное число неудачных попыток - по 2 попытки ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, VS-code, текстовый редактор и др.

Цель работы: Прочитать логи и найти ответ на вопрос

Критерий оценки: Предоставление правильного ответа

СЗИ-3 - Хронология событий (6/8) - 1 балл

Кажется сетевые атаки прекратились, но внутри деревни эйчаров заметили свинозомби! Надо выяснить что случилось, составив подробный ход событий атаки и ответить на вопросы CEO-старосты. Но не забывай, староста занятой, у тебя есть лишь несколько попыток для каждого ответа!

Вопрос от старосты: К какому хосту внутри сети злоумышленник пробрасывал доступ и на какой порт? Укажите в формате: ip:port.

ВАЖНО: Задание разбито на несколько отдельных вопросов, для ответа используется общий набор файлов логов. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют ограниченное число неудачных попыток - по 2 попытки ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, VS-code, текстовый редактор и др.

Цель работы: Прочитать логи и найти ответ на вопрос

Критерий оценки: Предоставление правильного ответа

СЗИ-3 - Хронология событий (7/8) - 1 балл

Кажется сетевые атаки прекратились, но внутри деревни эйчаров заметили свинозомби! Надо выяснить что случилось, составив подробный ход событий атаки и ответить на вопросы CEO-старосты. Но не забывай, староста занятой, у тебя есть лишь несколько попыток для каждого ответа!

Вопрос от старосты: К какой графической оболочке получил доступ злоумышленник?

ВАЖНО: Задание разбито на несколько отдельных вопросов, для ответа используется общий набор файлов логов. Необходимо ответить на вопросы в любом порядке с помощью формы сдачи флага на платформе. Вопросы имеют ограниченное число неудачных попыток - по 2 попытки ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, VS-code, текстовый редактор и др.

Цель работы: Прочитать логи и найти ответ на вопрос

Критерий оценки: Предоставление правильного ответа

СЗИ-3 - Хронология событий (8/8) - 1 балл

Кажется сетевые атаки прекратились, но внутри деревни эйчаров заметили свинозомби! Надо выяснить что случилось, составив подробный ход событий атаки и ответить на вопросы CEO-старосты. Но не забывай, староста занятой, у тебя есть лишь несколько попыток для каждого ответа!

Вопрос от старосты: Какой командой злоумышленник повысил привилегии на хосте hr?

ВАЖНО: Задание разбито на несколько отдельных вопросов, для ответа используется общий набор файлов логов. Необходимо ответить на вопросы в любом порядке с помощью формы

сдачи флага на платформе. Вопросы имеют ограниченное число неудачных попыток - по 2 попытки ответа на каждый вопрос! Ответ нужно сдавать без обертки.

Рекомендуемые утилиты: Libreoffice, VS-code, текстовый редактор и др.

Цель работы: Прочитать логи и найти ответ на вопрос

Критерий оценки: Предоставление правильного ответа