Задания 10 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 - Ловушка грифера (1/1) - 6 баллов

В подземельях нижнего мира грифер оставил редстоун-ловушку. Он принимает блоки и превращает их в зашифрованном виде, используя линейное заклинание над 64-битными блоками: C = (A * P + B) mod 2^64, где A - нечётное 64-битное число.

Формат флага: vsosh{...}

Рекомендуемые утилиты: netcat, python

Цель работы: Обезвредить ловушку грифера и расшифровать флаг за 2 запроса

Критерий оценки: Предоставление правильного флага

Web-1 - Коллекция морских огурцов (1/1) - 5 баллов

В тёплом океане ты нашёл коралловый риф, где местные жители собирают морские огурцы и обмениваются «сохранениями» — кто-то когда-то написал скрипт, который упаковывает коллекцию в особый формат. Загрузи своё сохранение, и сервер покажет, сколько в нём предметов. Говорят, в глубине рифа спрятан один особый экземпляр — тот, что светится секретом. В ходе разведки так же стало известно, что статические файлы раздаются из директории /app/static.

Рекомендуемые утилиты: Python, curl, Burp Suite

Цель работы: Добиться выполнения своего кода на сервере и получить флаг

Критерий оценки: Предоставление правильного флага

Web-2 - Ферма жителей (1/2) - 1 балл

В старой ферме жителей ты нашел сломанную редстоун схему. Исследуй схему внимательно - возможно, найдёшь какие-то пути, которые помогут в решении этой задачи

Рекомендуемые утилиты: burp suite, dirsearch, ffuf

Цель работы: Исследовать схему и найти флаг

Критерий оценки: Предоставление правильного флага

Web-2 - Ферма жителей (2/2) - 5 баллов

В старой ферме жителей ты нашел сломанную редстоун схему. Механизм должен ограничивать, какие данные могут изменять жители, но одна из воронок пропускает их! Изучи схему внимательно - возможно, ты сможешь изменить свою роль в этом механизме и найти путь в /admin.

Рекомендуемые утилиты: burp suite

Цель работы: Использовать ошибку в бизнес-логике и перейти в /admin

Критерий оценки: Предоставление правильного флага

Network-1 - Сеть двух баз Minecraft (1/3) - 1 балл

На карте мира Minecraft изображена сеть двух баз, соединённых через портал в Интернет: слева база Стива с локальным сервером SRV1 и роутерами R1–R3, а также отдельный дом Алекс (PC Alex), подключённый к роутеру R2. Справа — база Херобрина и Эндермена за роутером R4 и каскадом коммутаторов. Используя эту схему, ответьте на вопрос ниже.

Что нужно найти: наибольшую по размеру подсеть, которую можно назначить сети Стива так, чтобы диапазон адресов этой подсети не включал адреса ни одной другой сети или сегмента на схеме. Ответ укажите в формате /20.

Рекомендуемые утилиты: текстовый редактор, черновик для вычислений

Цель работы: определить допустимый префикс подсети по схеме адресации

Итог работы: корректно вписать ответ

Критерий оценки: предоставление корректного ответа

Network-1 - Сеть двух баз Minecraft (2/3) - 2 балла

На карте мира Minecraft справа расположена база Херобрина и Эндермена: ПК подключены к коммутатору SW TOP, который вместе с SW L и SW R образует треугольник из трёх коммутаторов. За SW R подключён роутер R4, через который база выходит в Интернет и далее может обращаться к другим узлам схемы.

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 подчёркивание в порядке возрастания, например: 1_3_5

Рекомендуемые утилиты: текстовый редактор, черновик для анализа таблиц коммутации и STP

Цель работы: проанализировать работу коммутаторов, STP и обучение MAC-адресов

Итог работы: корректно вписать ответ

Критерий оценки: предоставление корректного ответа

Network-1 - Сеть двух баз Minecraft (3/3) - 1 балл

Между двумя базами Minecraft поднят роутер R3, через который база Херобрина должна получать доступ к локальному веб-интерфейсу сервера Стива SRV1 (192.168.10.10). Снаружи R3 доступен по адресу 203.0.113.2, а сам веб-интерфейс работает по 443/tcp.

Войди на R3 по SSH и настрой его iptables так, чтобы: - входящие соединения на 203.0.113.2:443 перенаправлялись на 192.168.10.10:443 - доступ по этому правилу был разрешён только для публичного адреса R4 (203.0.113.6/32) - любые другие новые подключения к 203.0.113.2:443 оставались запрещёнными

В стенде уже настроены базовая маршрутизация, тестовые внешние узлы и сервис на стороне SRV1.

Рекомендуемые утилиты: ssh, bash, iptables

Цель работы: настроить корректное правило iptables

Итог работы: получить строку ответа от чекера

Критерий оценки: предоставление корректного флага

Forensics-1 - Бэкдор в процессе текстур-кэша (1/2) - 1 балл

После обнаружения DNS-туннеля администраторы провели аудит запущенных процессов и нашли подозрительный Python-скрипт, маскировавшийся под обновлятор кэша текстур. Админ снял дамп памяти через gcore.

Что нужно найти: URL-адрес вредоносного командного сервера (C2), с которым связывался бэкдор

Рекомендуемые утилиты: strings, grep

Цель работы: анализ дампа памяти процесса, поиск сетевых артефактов

Критерий оценки: предоставление корректного флага

Forensics-1 - Бэкдор в процессе текстур-кэша (2/2) - 1 балл

Адрес C2-сервера найден, но бэкдор не просто маячил — он собирал данные. В памяти процесса хранится конфигурация плагина, закодированная в base64. Внутри неё — украденный пароль администратора сервера.

Что нужно найти: украденный пароль администратора из base64-закодированного конфигурационного блока бэкдора

Рекомендуемые утилиты: strings, grep, base64, python3

Цель работы: обнаружение и декодирование скрытых конфигураций в дампе памяти

Критерий оценки: предоставление корректного флага

Forensics-2 - Утечка данных с сервера Pinecraft (1/3) - 1 балл

Во время Гранд-Турнира Pinecraft файрвол зафиксировал аномальные DNS-запросы, уходящие на неизвестный внешний хост. Администратор перехватил сетевой дамп. Похоже, один из серверных плагинов был троянизирован и тайно сливал данные наружу.

Что нужно найти: доменное имя C2-сервера, на который отправлялись подозрительные DNS-запросы

Рекомендуемые утилиты: Wireshark, tshark

Цель работы: анализ DNS-трафика, выявление аномальных доменов среди легитимных запросов

Критерий оценки: предоставление корректного флага

Forensics-2 - Утечка данных с сервера Pinecraft (2/3) - 1 балл

Командный сервер найден, но это только начало. Среди DNS-запросов к C2 есть серия странных поддоменных запросов — короткие hex-строки в качестве поддоменов. Это классический приём DNS-туннелирования: данные кодируются и прячутся прямо внутри доменных имён.

Вредоносный плагин разбил украденные данные на кусочки, закодировал каждый кусок в шестнадцатеричном формате и отправил как поддомен в DNS A-запросе. Собери все части и расшифруй послание.

Что нужно найти: декодированное содержимое данных, эксфильтрованных через DNS-туннель

Рекомендуемые утилиты: Wireshark, tshark, CyberChef, Python

Цель работы: извлечение и декодирование данных из DNS-туннеля (hex-encoded subdomains)

Критерий оценки: предоставление корректного флага

Forensics-2 - Утечка данных с сервера Pinecraft (3/3) - 1 балл

DNS-туннель был лишь частью атаки. В дампе обнаружился ещё один канал связи с C2-сервером — прямой HTTP-запрос с украденными данными. Среди них — токен администратора, с помощью которого атакующий может получить полный контроль над сервером.

Что нужно найти: токен администратора, украденный вредоносным плагином и отправленный на C2-сервер

Рекомендуемые утилиты: Wireshark, tshark, base64, Python

Цель работы: извлечение и анализ HTTP-трафика, декодирование base64-данных

Критерий оценки: предоставление корректного флага

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

Мистическое зло проникло в наши бухгалтерские архивы - работники не могут прочитать книги на столе выплат, жители бунтуют в ожидании изумрудов. Вирусный файл спрятался в системе, и его название неизвестно. Но мы знаем, что он там есть - злоумышленник зашифровал каталог и просит перевести изумруды.

Найдите название вирусного файла и пришлите его без расширения и обертки.

Рекомендуемые утилиты: volatility, strings, grep

Цель работы: Обнаружение названия вирусного файла

Критерий оценки: предоставление корректного флага

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

Мистическое зло проникло в наши бухгалтерские архивы - работники не могут прочитать книги на столе выплат, жители бунтуют в ожидании изумрудов. Вирусный файл спрятался в системе, и его название неизвестно. Но мы знаем, что он там есть - злоумышленник зашифровал каталог и просит перевести изумруды.

Найдите ID который был присвоен этому компьютеру и пришлите его без обертки.

Что нужно найти: ID компьютера

Рекомендуемые утилиты: volatility, strings, grep

Цель работы: Обнаружение ID компьютера

Критерий оценки: предоставление корректного флага-ID

Reverse-1 - AESвариус (1/1) - 3 балла

Таинственный житель-AESвариус отдал тебе странную книгу со словами "каждый может узнать содержимое". Постарайся понять, что за книга и как её прочитать, чтобы увидеть флаг.

Рекомендуемые утилиты: Ghidra, Python

Цель работы: Изучить алгоритм шифрования в книге и получить флаг из изображения

Критерий оценки: Предоставление правильного флага

Reverse-2 - Редстоуновый шеллкод (1/2) - 3 балла

Стив писал шеллкод. На редстоуне. Ключи внутри. Сам не помнит где. Ты понял.

Рекомендуемые утилиты: Ghidra, GDB, Python

Цель работы: Найти первый флаг внутри самодешифрующегося блока кода

Критерий оценки: Предоставление правильного флага

Reverse-2 - Редстоуновый шеллкод (2/2) - 3 балла

Стив писал шеллкод. На редстоуне. Ключи внутри. Сам не помнит где. Ну ты понял.

Рекомендуемые утилиты: Ghidra, GDB, Python

Цель работы: Найти второй флаг на основе первого внутри самодешифрующегося блока кода

Критерий оценки: Предоставление правильного флага

Pwn-1 - Quest Log (1/1) - 7 баллов

Стив устал от лагов сборщика мусора Java и написал менеджер квестов на C.

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

Цель работы: Поиск и эксплуатация уязвимости в бинарном приложении

Критерий оценки: Получение корректного флага

Privesc-1 - Капитальный баг (1/2) - 2 балла

Сегодняшняя смена в шахте началась с загадки. В сундуках вперемешку лежат кирки, таблички и старые карты, а на стене кто-то оставил надпись про второй ник. Кажется, это не просто склад, а база с чужими секретами.

Рекомендуемые утилиты: ssh, bash

Цель работы: Найти учетные данные и получить первый флаг

Критерий оценки: Предоставление правильного флага

Privesc-1 - Капитальный баг (2/2) - 3 балла

В туннелях ты слышишь тихое гудение редстоуна. Рядом с массивным сейфом висит табличка: «Не трогать механизмы». Но именно в них и спрятан путь к сердцу базы. Найди опасный баг в мисконфигурации и доберись до /root/flag2.txt.

Рекомендуемые утилиты: ssh, bash, getcap, setcap, cp

Цель работы: Получить второй флаг

Критерий оценки: Предоставление правильного флага

Misc-1 - Неразрушимый замок (1/1) - 3 балла

В деревне в общем хранилище лежит «замок» — файл, который не удаляется и не меняется обычными способами. Разберись, почему так выходит и как его убрать. Убери замок и запусти программу — она откроет сокровищницу и выведет флаг.

Рекомендуемые утилиты: ssh, rm, bash

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

Критерий оценки: Предоставление правильного флага

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

Поздравляем, тебя приняли главным смотрителем архивных дорог! В кибер-деревне сломались дорожные знаки на Nginx указателе, и запросы начали уводить к секретным свиткам. Беги чинить маршруты!

Рекомендуемые утилиты: ssh, nginx

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: Напишите название файла с конфигурацией VPN, который атакующий использовал для получение доступа во внутреннюю сеть организации? Файл нужно указывать без пути, с расширением.

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: Какие учетные данные мог использовать злоумышленник для авторизации на VPN?

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: Смог ли злоумышленник выполнить RCE на landing и повысить привилегии до root? Ответ сдавать в формате yes_yes/no_no/no_yes/yes_no.

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: Смог ли выполнить злоумышленник RCE на gitea и повысить привилегии до root? Ответ сдавать в формате no_no/ yes_yes/no_yes/yes_no.

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: Используя какого пользователя злоумышленник изменил репозиторий и какой файл он прочитал? Ответ в формате username_filename. Файл нужно указывать без пути, с расширением.

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 СЕО-старосты. Но не забывай, староста занятой, у тебя есть лишь несколько попыток для каждого ответа!

Вопрос от старосты: Какой файл отредактировал злоумышленник, чтобы повысить права на hr? Напишите полный путь до файла.

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 СЕО-старосты. Но не забывай, староста занятой, у тебя есть лишь несколько попыток для каждого ответа!

Вопрос от старосты: Укажите какие два файла очистил злоумышленник, чтобы замести следы? Ответ сдавать в формате полный-путь1_полный-путь2 (включая расширение, если есть).

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: Укажите какое ВПО загрузил злоумышленник, после повышения привилегий?

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