Задания 11 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 - Сундук с элитрами (1/1) - 6 баллов

В городах Края стоят эндер-сундуки с зашифрованными элитрами. Сундуки обмениваются ключами с помощью алгоритма Диффи-Хеллмана. Помоги достать элитры!

Формат флага: vsosh{...}

Рекомендуемые утилиты: netcat, python

Цель работы: Расшифровать флаг

Критерий оценки: Предоставление правильного флага

Web-1 - Коллекция морских огурцов (1/1) - 4 балла

В тёплом океане ты нашёл коралловый риф, где местные жители собирают морские огурцы и обмениваются «сохранениями». Пользователи могут не только загружать сохранения, но и создавать свои. При создании сервер упаковывает коллекцию и применяет какое-то странное шифрование. Доберись до светящегося секрета в глубине рифа. 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 - SP Monitor (1/2) - 1 балл

Появился новый мониторинг Minecraft-серверов. Операторы видят TPS, игроков и статус кластеров в реальном времени, а также умеют загружать моды прямо на сервер.

Рекомендуемые утилиты: burp suite, dirsearch, ffuf

Цель работы: Получить флаг

Критерий оценки: Предоставление правильного флага

Web-2 - SP Monitor (2/2) - 5 баллов

Появился новый мониторинг Minecraft-серверов. Операторы видят TPS, игроков и статус кластеров в реальном времени, а также умеют загружать моды прямо на сервер и хранить телеметрию серверов внутри Clickhouse.

Рекомендуемые утилиты: burp suite, curl

Цель работы: Получить флаг

Критерий оценки: Предоставление правильного флага

Network-1 - Сеть трех локаций Minecraft (1/3) - 1 балл

На карте мира Minecraft изображена сеть из трех локаций, связанных через Интернет-портал: слева — деревня Стива и Алекс, в центре — «серверная шахта» с выделенной серверной сетью и DMZ, справа — форпост Херобрина и Эндермена. Деревня подключена к порталу через роутер R1, серверная шахта выходит в Интернет через роутер R2, а форпост — через роутер R3. Между серверной шахтой (R2) и форпостом (R3) дополнительно поднят VPN-туннель для защищенного обмена данными между их внутренними сетями. Используя эту схему, ответьте на вопрос ниже.

Что нужно найти: наибольшую по размеру подсеть, которую можно назначить локальной сети деревни с хостами PC Steve и PC Alex, так, чтобы диапазон адресов этой подсети не включал адреса других сетей на схеме. Ответ укажите только в формате /24.

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 трех локаций Minecraft (2/3) - 2 балла

На карте мира Minecraft изображена сеть из трех локаций, связанных через Интернет-портал: слева — деревня Стива и Алекс, в центре — «серверная шахта» с выделенной серверной сетью и DMZ, справа — форпост Херобрина и Эндермена. Деревня подключена к порталу через роутер R1, серверная шахта выходит в Интернет через роутер R2, а форпост — через роутер R3. Между серверной шахтой (R2) и форпостом (R3) дополнительно поднят VPN-туннель для защищенного обмена данными между их внутренними сетями. Используя схему и приведенные ниже листинги, ответьте на вопрос.

Предположим, что VPN между R2 и R3 должен обеспечивать связность сети форпоста 192.168.40.0/24 с серверной сетью 192.168.20.0/24 и DMZ 192.168.30.0/24.

На маршрутизаторах 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, VPN, NAT и фильтрации

Цель работы: проанализировать роль VPN-туннеля, маршрутов, NAT и правил фильтрации между несколькими сетями

Итог работы: корректно вписать ответ

Критерий оценки: предоставление корректного ответа

Network-1 - Сеть трех локаций Minecraft (3/3) - 1 балл

Между серверной шахтой и форпостом Minecraft поднят VPN-туннель: серверная сеть и DMZ находятся за роутером R2, а сеть форпоста — за роутером R3. Через этот туннель форпост должен иметь ограниченный доступ к серверу в DMZ 192.168.30.10.

Войди на R2 по SSH и настрой его iptables так, чтобы: - из сети форпоста 192.168.40.0/24, приходящей через VPN, был разрешен доступ к 192.168.30.10 только по 22/tcp - разрешался только новый трафик по этому направлению - остальной новый трафик из сети форпоста в DMZ оставался запрещенным

В стенде уже настроены VPN-туннель, маршрутизация между подсетями и базовая политика защиты: FORWARD DROP, а также разрешен ESTABLISHED,RELATED.

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 - Скрытый канал в пингах Pinecraft (1/3) - 1 балл

Атакующий нашёл уязвимость в API управления плагинами и использовал её для закрепления на сервере. Мониторинг зафиксировал подозрительный всплеск HTTP-запросов. Админ снял дамп трафика.

Что нужно найти: URL эндпоинта (путь без параметров), который атакующий эксплуатировал через path traversal

Рекомендуемые утилиты: Wireshark, tshark

Цель работы: анализ сетевого трафика, обнаружение HTTP-запросов с path traversal

Критерий оценки: предоставление корректного флага

Forensics-1 - Скрытый канал в пингах Pinecraft (2/3) - 1 балл

Закрепившись на сервере, атакующий запустил инструмент эксфильтрации данных, маскирующий передачу под обычные пинги между нодами кластера. Среди ICMP-пакетов скрывается тайный канал с hex-кодированием.

Что нужно найти: данные, передаваемые через скрытый ICMP-канал (обратите внимание на поле ICMP Identifier)

Рекомендуемые утилиты: Wireshark, tshark, Python, CyberChef

Цель работы: анализ ICMP-трафика, декодирование hex-полезной нагрузки

Критерий оценки: предоставление корректного флага

Forensics-1 - Скрытый канал в пингах Pinecraft (3/3) - 1 балл

Помимо hex-канала, атакующий настроил второй, зашифрованный канал эксфильтрации через ICMP. Этот канал использует другой идентификатор и XOR-шифрование. Ключ шифрования спрятан где-то в том же дампе трафика — внимательно изучи HTTP-ответы сервера.

Что нужно найти: данные из зашифрованного ICMP-канала (найдите ключ в HTTP-трафике и расшифруйте XOR)

Рекомендуемые утилиты: Wireshark, tshark, Python

Цель работы: обнаружение XOR-ключа в HTTP-заголовках, дешифрование скрытого канала

Критерий оценки: предоставление корректного флага

Forensics-2 - PineLocker — Последний удар (1/3) - 1 балл

Перед побегом атакующий запустил на сервере самодельный шифровальщик PineLocker. Все конфигурационные файлы сервера превратились в нечитаемый мусор, появилась записка с требованием выкупа в 64 алмазных блока. Администратор снял образ диска.

Что нужно найти: первые 12 символов SHA256-хеша скрипта шифровальщика .pinelocker.py

Рекомендуемые утилиты: mount, find, sha256sum

Цель работы: монтирование образа диска, поиск скрытых файлов, вычисление хешей

Критерий оценки: предоставление корректного флага

Forensics-2 - PineLocker — Последний удар (2/3) - 1 балл

Скрипт шифровальщика найден, но для расшифровки файлов нужен ключ. Атакующий действовал в спешке и не позаботился о заметании всех следов. Где-то в системе остались улики — история его действий может содержать ответ.

Что нужно найти: ключ шифрования, использованный при запуске PineLocker

Рекомендуемые утилиты: mount, cat, grep, strings

Цель работы: исследование артефактов командной оболочки в файловой системе

Критерий оценки: предоставление корректного флага

Forensics-2 - PineLocker — Последний удар (3/3) - 1 балл

Скрипт и ключ найдены. Среди зашифрованных файлов есть server.properties.locked — главный конфигурационный файл Minecraft-сервера. Изучите алгоритм шифрования в .pinelocker.py, напишите дешифратор и восстановите содержимое. Найдите значение параметра admin-secret.

Что нужно найти: значение параметра admin-secret из расшифрованного server.properties

Рекомендуемые утилиты: Python 3

Цель работы: реверс-инжиниринг алгоритма шифрования, написание дешифратора

Критерий оценки: предоставление корректного флага

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

Мистическое зло проникло в наши архивы через редстоун-сеть - оно требует изумрудов. Но ты то не зря 30 уровень фармил, сможешь провести анализ? Нужно узнать какой файл запустил цепочку атаки (он все еще в памяти). Сдай название этого файла 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 архивы - оно требует изумрудов. Но ты то не зря 30 уровень фармил, сможешь провести анализ? Что именно использовал бинарь для повышения привилегий (говорят, это связано с объектами) и какой ID у этого объекта в Windows? Формат флага - повышение_ID. Пришли его без обертки.

Рекомендуемые утилиты: volatility, ghidra, strings, grep

Цель работы: Исследование вредоносного файла и обнаружение способа повышения привилегий и ID объекта для повышения привилегий

Критерий оценки: предоставление корректного флага - повышение_ID

Reverse-1 - VPN для бариста (1/1) - 3 балла

В одном из сундуков жителя-бариста, я нашел интересную пластинку для доступа к удаленному проигрывателю, но она у меня постоянно вылетает. Сможешь посмотреть почему?

Рекомендуемые утилиты: Jadx, Ghidra

Цель работы: Изучить библиотеку странной функции и получить флаг

Критерий оценки: Предоставление правильного флага

Reverse-2 - Куриный фристайл (1/2) - 3 балла

Как то раз Стив вернулся из пещер и увидел вечеринку на его мини-ферме. Но в движении куриц было что-то очень неуловимо странное... Надо бы понять секрет их классных движений.

Рекомендуемые утилиты: Ghidra, GDB, Python

Цель работы: Найти первый флаг

Критерий оценки: Предоставление правильного флага

Reverse-2 - Куриный фристайл (2/2) - 3 балла

Как то раз Стив вернулся из пещер и увидел вечеринку на его мини-ферме. Но в движении куриц было что-то очень неуловимо странное... Стив узнал секрет, побей его рекорд.

Рекомендуемые утилиты: Ghidra, GDB, Python

Цель работы: Найти второй флаг, побив рекорд Стива

Критерий оценки: Предоставление правильного флага

Pwn-1 - Enchantment Table (1/1) - 7 баллов

Стив написал систему зачарований на C, чтобы не забывать какие чары уже нанесены.

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

Цель работы: Поиск и эксплуатация уязвимости в бинарном приложении

Критерий оценки: Получение корректного флага

Privesc-1 - Поднять сервер (1/2) - 2 балла

В шахте Стива стоит ферма слизней. Рядом - сундуки с заметками и книжками, где он записывал координаты чанков и порталов.

Рекомендуемые утилиты: ssh, bash

Цель работы: Найти учетные данные и получить первый флаг

Критерий оценки: Предоставление правильного флага

Privesc-1 - Поднять сервер (2/2) - 3 балла

Алекс строит свою базу с помощью схематики, но в её конфигурации была допущена критическая ошибка. Используй её, чтобы достать флаг из сундука в /root/flag.txt.

Рекомендуемые утилиты: ssh, bash, sudo, ansible-playbook

Цель работы: Получить второй флаг

Критерий оценки: Предоставление правильного флага

Misc-1 - Сейф с кодом (1/1) - 3 балла

В подземелье деревни нашли запечатанный сейф: внутри — механизм, который принимает код. Если код верный, сейф отдаёт сокровище. Правильный код знает только хранитель сокровищницы, в общем доступе его нет. При неверном коде механизм перемещается, а рядом с ним всегда лежит куча мусора. Попадите в сокровищницу и получите флаг.

Рекомендуемые утилиты: ssh, bash

Цель работы: Получить флаг из сокровищницы.

Критерий оценки: Предоставление правильного флага

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

Поздравляем, тебя назначили старшим по паспортному контролю. В деревне нашли поддельные цифровые пропуска, и теперь любой может пройти в закрытую зону.

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 менеджеров 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 endpoint на landing позволил злоумышленнику получить доступ во внутреннюю сеть? Укажите в формате /path/to/endpoint.

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 - 1 попытка 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 менеджеров 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: С помощью какой команды злоумышленник выбрался из контейнера? Напишите точную команду со всеми аргументами

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 - 1 попытка 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 менеджеров 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 хост gitea и повысить там привилегии? 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 - 1 попытка 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 менеджеров 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: Прочитав какой файл злоумышленник смог развить атаку в windows сегмент? 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 - 1 попытка 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 менеджеров 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 какой протокол злоумышленник смог получить доступ к компьютеру директора? Укажите название протокола.

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 - 1 попытка 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 менеджеров 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: С помощью какого исполняемого файла злоумышленник повысил привилегии на хосте директора? 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 - 1 попытка 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 менеджеров 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 полный путь до файла, с которым злоумышленник повысил привилегии на dc-01.

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 - 1 попытка 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 менеджеров 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 в какие файлы злоумышленник сохранил чувствительные данные системы, после повышения. Укажите имена файлов через _. Пример: temp.txt_temp2.txt

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 - 1 попытка 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