

Заключительный этап

Первый тур заключительного этапа

Первый тур заключительного этапа прошел на специальной платформе в формате CTF task-based с добавлением творческих задач.

Особенности тура:

- Длительность тура: 4 астрономических часа.
- Интернет отсутствует.
- Для каждого участника был подготовлен ноутбук с предустановленной ОС Kali Linux 2022.4
- Каждая задача по категориям оценивалась в 10 баллов.
- Платформа хостилась на локальной сети Университета, что ограничивало поиск подсказок в сети интернет.

Творческие задания оценивались по шкале от 0 до 20 баллов с шагом 2 балла в задачах Incident Manager и Квантовое шифрование, задачи Виженер и AND or OR решались на выданных бланках и оценивались по шкале от 0 до 15 баллов с шагом в 5 баллов.

Задачи первого тура заключительного этапа

1. Творческое

1.1. Квантовое шифрование

Балл: 20

Условие:

В последние годы область квантового шифрования претерпела значительные изменения, став одним из наиболее обсуждаемых направлений в информационной безопасности. Квантовое шифрование использует принципы квантовой механики для обеспечения безопасности передачи информации, что теоретически делает её невосприимчивой к взлому с помощью классических и даже квантовых вычислений.

Задание:

Ваша задача — провести анализ перспектив, пользы и угроз, связанных с применением квантового шифрования в информационной безопасности. Ваш ответ должен включать следующие аспекты:

Перспективы развития квантового шифрования:

Оцените потенциал квантового шифрования и его возможное влияние на будущее информационной безопасности.

Проанализируйте, какие технологические и теоретические проблемы ещё предстоит решить.

Польза квантового шифрования:

Опишите, как квантовое шифрование может улучшить защиту данных и коммуникаций.

Приведите примеры областей применения, где квантовое шифрование могло бы принести наибольшую пользу.

Угрозы и вызовы, связанные с квантовым шифрованием:

Рассмотрите потенциальные угрозы, которые квантовое шифрование может представлять для существующих систем безопасности.

Обсудите, какие вызовы стоят перед обществом и специалистами в области информационной безопасности при внедрении квантовых технологий.

1.2. Incident manager

Балл: 20

Условие:

Задание:

Вводные данные:

Вы - инцидент менеджер в крупной компании.

За каждым подразделением (условный юнит компании, такие как бухгалтерия, сетевики, отдел продаж) закреплено свое ответственное лицо. Бекапы критичных серверов делаются раз в месяц. Высшее руководство компании улетело на корпоратив всем составом, так что фактически вы можете принимать любые решения. Через несколько дней наступит сразу два важных события: выдача зарплаты сотрудникам и период финансового отчета перед поставщиками продукции для вашей фирмы.

В один прекрасный (нет) день вам приходит уведомление, что на серверах 1с расширения файлов начали меняться, а также в корне диска появился файл следующего содержания <типичный текст шифровальщика вставляю>. Тут же один из бухгалтеров вспоминает, что какое-то время назад ей на почту приходило странно письмо с документом, после открытия которого «что-то быстро моргнуло».

Ваша задача описать весь процесс реактивного реагирования и митигации последствий с точки зрения инцидент-менеджера, с указанием какие дополнительные службы/источники/внешние фирмы вы будете привлекать и для каких целей

2. Paper

2.1. AND or OR?

Балл: 15

Условие:

Составьте таблицу истинности для следующего логического выражения:

$$F(X, Y, Z) = (X \wedge \neg Y) \vee (Y \wedge Z) \vee (\neg X \wedge \neg Z)$$

Здесь используются следующие логические операции:

- \wedge — логическое И (AND),
- \vee — логическое ИЛИ (OR),
- \neg — логическое НЕ (NOT).

Вам необходимо построить таблицу истинности для данного выражения, учитывая все возможные комбинации значений переменных X, Y и Z которые могут быть либо 0 (ложь), либо 1 (истина).

2.2. Вижнер

Балл: 15

Условие:

Вам необходимо с помощью представленной ниже таблицы и шифра Виженера выполнить две задачи:

Зашифровать фразу «ctf its easy» с ключевой фразой «some key».

Расшифровать фразу «kmx c lnoiqg onixsgk hkingk» используя ключевую фразу «ctf».

Так же необходимо описать алгоритм и представить псевдо-код программы, позволяющей производить шифрование/дешифрование произвольной фразы с указанием ключа.

3. Web

3.1. GetTheFile

Балл: 10

Условие:

Just read file and get your points!

<http://10.90.138.119:5555>

4. PWN

4.1. ha-ha, classic

Балл: 10

Условие:

It's just classic pwn task!

nc 10.90.138.119 5050

5. Forensic

5.1. hacker

Балл: 10

Условие:

My computer was hacked! I just get some strange file from hacker and message "try to find me, friend". Can you help me?

6. Reverse

6.1. Slowly

Балл: 10

Условие:

This code is so slowly... But i very need flag!

7. Network

7.1. Двойное рукопожатие

Балл: 10

Условие:

Наш сервер слушает порт 31337. Если вы подключаетесь только одним способом, то в ответ - тишина. Если же подключаться по правильной схеме, а-ля port-knocking, то сервер вам обязательно ответит. Я еще не разобрался в комбинации, но у других коллег это получалось. Сейчас суббота, они недоступны... помогите!!!

8. Misc

8.1. file

Балл: 10

Условие:

Файл без опознавательных знаков был замечен на компьютере главного бухгалтера. Узнайте, что было спрятано, и являются ли эти данные критичными?

9. PPC

9.1. печь

Балл: 10

Условие:

на вход вам дана последовательность слов, в ответ необходимо отправить количество глаголов (в инфинитиве). Раундов будет много.

В случае, если слово является существительным и глаголом, используется вариант глагол (например, печь).