Задание от партнера олимпиады — ПАО «ФосАгро»

1. Сетевая безопасность

Задание 1.1. Анализ сетевых атак

Ситуация: В локальной школе участились случаи замедления интернета. Подозревают DDoS-атаку.

Вопросы:

1. Объясните, как отличить DDoS-атаку от обычной перегрузки сети.
2. Какие меры можно принять для защиты?

Назовите 3 способа.

Задание 1.2. Настройка межсетевого экрана

Даны правила фаервола:

plaintext

1. Разрешить входящие HTTP/HTTPS.
2. Запретить все входящие подключения с IP 192.168.1.100.
3. Разрешить исходящие подключения на порт 53 (DNS).

Вопрос: Какие уязвимости остались в этих правилах?

Предложите 2 исправления.

2. Управление уязвимостями

Задание 2.1. Приоритезация угроз

Даны уязвимости системы:

- CVE-2023-1234 (критическая, позволяет удаленный запуск кода).
- CVE-2023-5678 (средняя, утечка информации).
- CVE-2023-9012 (низкая, ошибка интерфейса).

Вопрос: В каком порядке их нужно исправлять? Обоснуйте.

Задание 2.2. Анализ обновлений

Ситуация: Выпущен патч для ОС, но его установка требует перезагрузки сервера, который работает 24/7.

Вопрос: Какие риски возникают при установке и отказе от патча? Предложите компромиссное решение.

Задание от партнера олимпиады — ПАО «ФосАгро»

3. Анализ вредоносного ПО

Задание 3.1. Исследование поведения

Описание:

Программа при запуске:- Создает файл C:\temp\keylog.txt.- Подключается к IP 10.0.0.5 через порт 4444.

Вопрос: Какой тип угрозы это может быть? Какие данные находятся в зоне риска?

Задание 3.2. Статический анализ

Дана строка из подозрительного файла:

Start-Process -FilePath "cmd.exe" -ArgumentList "/c shutdown /s /t 0"

Вопрос: Что делает этот код? Как защититься от таких скриптов?

4. Политики безопасности и стандарты

Задание 4.1. Разработка политики паролей

Требуется: Создать правила для паролей в компании, учитывая: минимальную длину, использование символов и частоту смены.

Вопрос: Напишите 5 пунктов политики и объясните их важность.

Задание 4.2. Работа с инцидентами

Ситуация: Сотрудник потерял USB-накопитель с конфиденциальными данными.

Вопрос: Какие шаги должны быть предприняты согласно политике безопасности?

5. Криптография и защита данных

Задание 5.1. Асимметричное шифрование

Вопрос: Почему для HTTPS используется связка RSA и AES? Объясните роль каждого алгоритма.

Задание 5.2. Хэширование

Даны хэши паролей:

- 5f4dcc3b5aa765d61d8327deb882cf99 (MD5)
- a94a8fe5ccb19ba61c4c0873d391e987982fbbd3 (SHA-1)

Вопрос: Почему MD5 и SHA-1 считаются ненадежными? Приведите пример атаки.

Задание от партнера олимпиады — ПАО «ФосАгро»

6. Практические симуляции

Задание 6.1. Сканирование сети

Инструмент: Nmap (условно).

Задача: Определить открытые порты на IP 192.168.1.1. Напишите команду и объясните, какие порты могут быть уязвимы (например, порт 22 — SSH).

Задание 6.2. Анализ логов

Дан фрагмент лога веб-сервера:

plaintext

192.168.1.15 - - [01/Jan/2023] "GET /wp-admin.php HTTP/1.1" 404

192.168.1.15 - - [01/Jan/2023] "POST /login.php HTTP/1.1" 200

Вопрос: Какие признаки атаки здесь видны?

7. Этические и правовые аспекты

Задание 7.1. Кейс по киберпреступности

Ситуация: Хакер взломал сайт магазина, но не украл данные, а сообщил администратору об уязвимости.

Вопрос: Можно ли считать его действия законными? Какие правовые нормы регулируют такие случаи?

8. Творческие задачи

Задание 8.1. Создание схемы защиты

Задача: Нарисуйте схему защиты домашней сети, включив: роутер, ПК, IoT-устройства, фаервол, антивирус. Подпишите угрозы для каждого элемента.

Задание 8.2. Ролевая игра

Сценарий: Один участник —«атакующий» (пытается объяснить метод взлома), второй — «защитник» (предлагает контрмеры).

Тема: Фишинг vs. Обучение сотрудников.