**Теоретическая часть**

Что такое вредоносное ПО (вирусы, трояны, вымогатели)? Принцип их работы

|  |  |  |
| --- | --- | --- |
| Тип вредоносного ПО | Описание | Принцип работы |
| **Вирусы** | Самораспространяющиеся программы, внедряющиеся в другие файлы или системы | Вирусы прикрепляются к файлам или загрузчикам, активируются при запуске, могут копировать себя, повреждать файлы или системы |
| **Трояны** | Маскируются под легитимные программы, скрываясь внутри них | Пользователь запускает "легитимную" программу, которая в фоновом режиме выполняет вредоносные действия, например, открывает доступ злоумышленникам |
| **Вымогатели (Ransomware)** | Шифруют файлы или блокируют доступ к системе, требуют выкуп | Вредоносное ПО шифрует данные или блокирует систему, после чего требует оплату за восстановление доступа |

***Принципы анализа вредоносного ПО***

***Статический анализ (без запуска)***

- Анализ исходного кода или бинарных файлов без их выполнения

- Использует инструменты для изучения структуры файла, поиска вредоносных сигнатур, обфускации, строк, ресурсов

- Цель: выявить признаки вредоносной активности, определить функциональность

***Динамический анализ (с запуском)***

- Анализ поведения программы в контролируемой среде

- Мониторинг системных вызовов, файловых операций, сетевых соединений, изменений реестра

- Использует инструменты типа Process Monitor, FakeNet, виртуальные машины

***Основные правила безопасности при исследовании ВПО***

- Использовать изолированную среду (виртуальные машины, песочницы)

- Не запускать вредоносное ПО на основном рабочем компьютере

- Отключать сеть или использовать изолированные сети

- Делать резервные копии данных

- Использовать антивирусные и антивредоносные инструменты

- Вести журнал действий и сохранять образ системы для анализа

---

**Практические задания**

**Таблица результатов**

|  |  |  |  |
| --- | --- | --- | --- |
| Образец | Создает файлы | Меняет реестр | Сетевые запросы |
| eicar.com | Нет | Нет | Нет |
| game.exe | Нет | Нет | Да (на example.com) |

**Ответы на вопросы**

1. Какие признаки вредоносного поведения вы обнаружили?

Отсутствие признаков вредоносных действий у eicar.com, у трояна — сетевые соединения и чтение файла.

2. Почему EICAR безопасен для анализа?

Он предназначен для тестирования антивирусных решений и не содержит вредоносных функций.

3. Как FakeNet помогает анализировать сетевую активность?

Создает виртуальную среду для перехвата и логирования сетевых запросов, позволяя выявить попытки связи вредоносных программ.

4. Что такое вредоносное программное обеспечение (ВПО) и какие его основные типы?

Программное обеспечение, наносящее вред системе или пользователю: вирусы, трояны, вымогатели, черви, руткиты.

5. Каковы основные цели анализа вредоносного ПО?

Выявление функциональности, понимание механизмов, разработка методов защиты, обнаружение уязвимостей.

6. В чем заключается разница между статическим и динамическим анализом?

Статический — без запуска, по коду; динамический — при выполнении, по поведению.

7. Какие инструменты наиболее распространены для статического анализа?

Ghidra, IDA Pro, Radare2 — для дизассемблирования и анализа бинарных файлов.

8. Что такое обфускация кода?

Процесс усложнения исходного кода для затруднения анализа, используется для скрытия вредоносных функций.

9. Признаки наличия вредоносного кода?

Необычные сетевые соединения, изменение реестра, создание/удаление файлов, запуск скрытых процессов.

10. Что такое песочница (sandbox)?

Изолированная среда для безопасного анализа вредоносных программ.

11. Методы обхода антивирусов?

Обфускация, использование загрузчиков, код-обфускация, внедрение в доверенные процессы.

12. Что такое инъекция кода?

Внедрение вредоносного кода в процессы или память других программ для маскировки или выполнения атак.

13. Этапы динамического анализа?

Запуск программы, мониторинг системных вызовов, сетевых соединений, изменений системы.

14. Что можно извлечь при статическом анализе?

Строки, ресурсы, структура файла, функции, признаки обфускации.

15. Как помогает изучение поведения?

Позволяет выявить реальные действия вредоносной программы, разработать защитные меры.

16. Распространенные сценарии использования ВПО?

Кража данных, шпионаж, вымогательство, распространение через сети.

17. Что такое reverse engineering?

Обратная разработка — анализ и восстановление исходного кода или логики программы.

18. Риски анализа в реальной среде?

Инфекция системы, утечка данных, распространение вредоносных компонентов.

19. Меры предосторожности?

Использование изолированных сред, резервных копий, антивирусных решений.

20. Как помогает анализ в расследованиях?

Обнаружение методов атаки, выявление источников, разработка контрмер.

21. Этические аспекты?

Соблюдение законодательства, конфиденциальность, ответственность за использование данных.