**Все работы выполняются строго на виртуальных стендах, созданных в безопасной и изолированной среде.**
**Запрещается использование разработанных программ вне установленной учебной среды.**

**Цель проекта**: создание лабораторного стенда для безопасного изучения подозрительного ПО.

**Задачи**:

- настройка лабораторного стенда с использованием гипервизора,
- демонстрация работы ВПО, - подробный анализ функционала ВПО,
- описание и реализация мер защиты от ВПО.

Задание по вариантам:

| | 3.8.B.1 | 3.8.B2 | 3.8.B.3 |
|---|---|---|---|
| Файл | Sample-1.exe | Sample-2.exe | Sample-3.exe |

**Используемое ПО:**

- VMWare – для разворачивания виртуальной сети,
- Windows 10 – машина администратора сети (с нее будет проводиться обнаружение атаки),
- FLARE-VM — набор сценариев установки программного обеспечения для систем Windows,
- PeStudio — инструмент, который сканирует программы в поисках релевантной информации, строковых значений и ресурсов и отображает всю собранную после анализа информацию,
- IDA Pro – интерактивный дизассемблер,
- Dependensy Walker – ПО, используемое для получения списка импортируемых и экспортируемых функций PE-файла,
- Process Hacker – утилита для мониторинга системных процессов и служб Windows,
- Process Explorer – приложение для мониторинга процессов в системе,
- RegShot – утилита сравнения реестра,

- Wireshark – анализатор трафика для компьютерных сетей,
- OBS Studio – для записи видео демонстрации атаки, - Power Point – для подготовки презентации.

**Минимальные требования:**

- Оперативная память – 8 ГБ,
- Свободное дисковое пространство – 250 ГБ.

**Этапы исследования**:

1) Изучение ПО VMWare. Интерфейс программы, функции, его возможности.
2) Установка необходимого ПО на VMWare.
3) Изучение методов изоляции виртуальных машин от основного хоста.
4) Изучение FLARE-VM. Установка.
5) Настройка стенда.
6) Изучение структуры исполняемого файла.
7) Изучение разновидностей ВПО.
8) Изучение методов анализа ВПО. Статический и динамический анализ.
9) Изучение ПО для анализа ВПО.
10) Выбор экземпляра ВПО.
11) Методы защиты от ВПО. Способы реализации. Демонстрация работы.
12) Подготовка лабораторного стенда к демонстрации анализа ВПО.
13) Подготовка презентации по проделанной работе, доклада и краткого содержания работы.

**Результаты, рекомендации, возможное решение проблем**: результаты проекта включают в себя готовый лабораторный стенд, который защищен от воздействия ВПО на основной хост, результаты анализа ВПО, его основной функционал, презентация (см. требования к презентации) и отчет по выполненному проекту (см. требования к отчету).

Рекомендации к составу отчета:

1) Содержание
2) Задание с указанием варианта

3) Описание лабораторного стенда
4) Статический анализ вируса
5) Динамический анализ вируса
6) Методы защиты от вируса
7) Заключение
8) Список использованных источников

**Требования к презентации и защите:**

- Количество слайдов: 15-20 слайдов,
- Обязательными разделами презентации должны быть:
  1) Титульный лист с представлением названия проекта и состава подгруппы.
  2) Цель, задачи проекта.
  3) Этапы реализации проекта с предоставлениями промежуточных результатов.
  4) Результат проекта.
- Все слайды должны быть сделаны в двух-трех основных цветах, которые гармонируют между собой.
- Текст должен хорошо читаться даже с дальних мест.
- Изображения и анимация должны быть хорошего качества.
- Каждый слайд должен иметь заголовок, несущий информацию о его содержании.
- Проект к защите допускается преподавателем только при возможности демонстрации готового решения.
- Защита проекта длится 25 минут. В защите участвуют все студенты подгруппы, где каждому из них выделяется по 5 минут.

**Требования к отчету:**

Отчет оформляется в соответствии с требованиями, предъявленными к выпускным квалификационным работам согласно методическим указаниям по написанию, оформлению и защите выпускных квалификационных работ.

Отчет по проекту имеет следующую структуру:

- задание,
- титульный лист,
- содержание,

-текст работы, структурированный по главам,

-заключение,

-список использованных источников, -приложения

(при необходимости).

Общий объем отчета не должен превышать 30 страниц без приложений. Работа должна быть напечатана на одной стороне листа белой бумаги форматом А4. Рекомендуемый шрифт Times New Roman, размер 14, межстрочный интервал – 1,5. Текст работы следует печатать, соблюдая следующие размеры полей: левое – 30 мм, правое – 10 мм, верхнее – 20 мм, нижнее – 20 мм. Следует включить режим выравнивание по ширине. Все страницы должны быть пронумерованы, кроме титульного листа, и содержания. Задание необходимо распечатать и скрепить отдельно.

Титульный лист должен содержать полное наименование вуза, название подразделения (факультет, кафедра), в котором выполнена работа, название проекта, фамилии, имена, отчества авторов, наименование места и год выполнения.

Содержание представляет собой составленный в последовательном порядке список всех заголовков разделов работы с указанием страниц, на которых соответствующий раздел начинается.

Во введении отчета (рекомендуемый объем не более 1-2 страниц) – делается краткое описание проекта, его целей и задач, а также полученных результатов. Также необходимо указать роли, которые студенты подгруппы выполняли при реализации проекта.

Основная часть отчета должна содержать главы в соответствии с этапами реализации проекта. Каждая глава должна содержать описание этапа, его задачи, промежуточные результаты, описание выполненных работ, анализ возникающих проблем и путей их решения.

В заключении необходимо суммировать результаты проекта, соотнести их с планируемыми результатами, дать краткую оценку в целом всему проекту.

Приложения должны включать вспомогательный или дополнительный материал, который загромождает текст основной части работы, но необходим для полноты ее восприятия и оценки практической значимости.

На всех иллюстрациях должно быть четко видно актуальную дату и время как на компьютере хоста, так и на виртуальной машине. Они должны совпадать.

**Список литературы:**


1. Статический анализ кода|PVS-Studio [Электронный ресурс]. Режим доступа: https://pvs-studio.ru/ru/blog/terms/0046/ - статический анализ кода

2. Вскрытие покажет! Практический анализ вредоносного ПО. — СПб.: Питер, 2018. — 768 с.

3. Компьютерные вирусы и вредоносное ПО: факты и часто задаваемые вопросы [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malwarefacts-and-faqs - компьютерные вирусы и вредоносное ПО

4. Как создать виртуальную машину VMware Workstation и установить на неё Windows [Электронный ресурс]. https://www.white-windows.ru/kaksozdat-virtualnuyu-mashinu-vmware-workstation-i-ustanovit-na-neyowindows/?ysclid=lrhkqbnbjd622860475 – установка windows на vmware