Домашнее задание

Дисциплина: Программирование на Python
Тема: Python для аналитиков ИБ: форензика

Форма проверки: самопроверка
Имя преподавателя: Денис Алмакаев
Время выполнения: 180 минут

Цель задания:

- Ознакомиться с инструментами цифровой криминалистики (форензики) и получить практический опыт анализа дампов памяти или сетевых дампов.
- Научиться извлекать ключевые артефакты (процессы, соединения, DNS-запросы) и представлять результаты анализа.

Инструменты для выполнения ДЗ:
volatility, pyshark, Matplotlib, Seaborn, IDE PyCharm или VSCode, репозиторий на GitHub

Правила приёма работы:

1. Выполните все пункты задания.
2. Разместите готовый код и визуализацию в репозитории на GitHub.
3. В личном кабинете, в поле ответа к домашней работе, вставьте ссылку на GitHub-репозиторий.
4. Отправьте работу на проверку. Важно: убедитесь, что по ссылке есть доступ.

Критерии оценки:

Задание считается выполненным:

- прикреплена ссылка на репозиторий с выполненным заданием,
- доступ к репозиторию открыт,
- коды выдают правильные ответы к задачам.

Задание считается невыполненным:

- ссылка на репозиторий с заданием не прикреплена или закрыт доступ по ссылке,
- коды выдают ошибку или неправильные ответы.

Дедлайн: 7 дней после соответствующего вебинара.

Прежде чем выполнять домашнее задание:

1. Посмотрите запись вебинара по теме «Python для аналитиков ИБ: форензика».
2. Установите необходимые библиотеки и инструменты. Убедитесь, что в вашем рабочем окружении Python установлены библиотеки **pyshark**, а также инструмент **volatility** для анализа дампов.
   Если нет, установите их с помощью pip и инструкции по установке volatility:

pip install pyshark

Задание

Загрузите дамп памяти или дамп сети. Вы можете использовать предоставленный дамп сети или найти тестовые дампы сети / памяти, например, из открытых учебных примеров
Найдите ключевые артефакты: процессы, соединения, DNS-запросы.

Этап 1. Загрузка данных
Скачайте или используйте предоставленный дамп памяти или дамп сети.
Важно: можно использовать тестовые дампы, например, из открытых учебных примеров.

Этап 2. Извлечение ключевых артефактов
В зависимости от выбранного типа дампа:

- Если работаете с дампом памяти, с помощью **volatility** получите список активных процессов и сетевых соединений.
- Если работаете с дампом сети, с помощью **pyshark** выделите DNS-запросы, IP-адреса и другие значимые события.

Этап 3. Визуализация результатов
Создайте минимальную визуализацию или лог. Например:

- таблицу или список с именами процессов, временем их запуска;
- список подозрительных IP-адресов и доменов;
- график количества DNS-запросов по времени.

Можно использовать **Matplotlib**, **Seaborn** или сохранить результаты в формате .csv или .json.

Чек-лист самопроверки

Критерии выполнения лабораторной работы
Установлены необходимые библиотеки и инструменты: volatility и/или pyshark
Дамп памяти или дамп сети успешно загружен
С помощью volatility или pyshark получены ключевые артефакты: имена процессов, IP-адреса, DNS-запросы
Создана минимальная визуализация или лог с результатами анализа
Результат выполнения лабораторной работы соответствует требованиям задания
На учебной платформе прикреплена ссылка на GitHub-репозиторий с кодом
Репозиторий по ссылке доступен для просмотра другим пользователям, название репозитория содержит фамилию и имя студента, номер лабораторной работы