Домашнее задание

Дисциплина	Технологии детектирования атак и управления инцидентами
Тема	Анализ дампа ОЗУ
Форма проверки	**Самопроверка. Студент выполняет задание и получает правильные ответы после дедлайна**
Имя преподавателя	Михаил Николаев
Время выполнения	60 минут
Цель задания	Получение навыков поиска, обработки и анализа криминалистических артефактов на уровне дампа оперативной памяти
Инструменты для выполнения ДЗ	Volatility, Google Doc / Яндекс документы
Правила приёма работы	1. Выполните все пункты задания. 2. Подготовьте файл с ответами на вопросы. 3. Загрузите файл на Google Диск и прикрепите ссылку на файл с выполненным заданием в LMS. Важно: убедитесь, что по ссылке есть доступ. Название файла должно содержать фамилию и имя студента, номер ДЗ
Критерии оценки	**Задание считается выполненным, если:** • прикреплена ссылка на файл с выполненным заданием; • доступ к материалам открыт. **Задание не выполнено, если:** • файл с заданием не прикреплён или отсутствует доступ по ссылке
Дедлайн	7 дней после вебинара

Описание задания

Перед тем, как выполнить задание:

- посмотрите запись вебинара «Анализ дампа ОЗУ»;

- разверните образ виртуальной машины на локальном хосте слушателя. Как это сделать — описано в гайде, он есть в архиве. Для этого пройдите по ссылке https://cloud.f6.ru/s/9AFym78c2DQD2Jz. Пароль: 3809659233693;
- используйте инструмент Volatility и изученные на вебинаре плагины.

Этап 1.
Проанализируйте дамп памяти Incident.mem.

Этап 2.
Используя утилиту Volatility и изученные на вебинаре плагины, ответьте на вопросы:

1. Когда был снят дамп? (UTC)
2. Какая версия операционной системы, с которой был снят дамп?
3. Каково количество запущенных процессов?
4. Какой родительский идентификатор процесса powershell.exe?
5. Какое имя процесса, «слушающего» порт 3389?
6. Какой идентификатор процесса, который встречается в выводе плагина malfind 5 раз?
7. Когда в последний раз выключалась система? (UTC)

Этап 3.

Подготовьте файл с ответами на вопросы. Загрузите файл на Google Диск / Яндекс диск и прикрепите ссылку на файл с выполненным заданием в LMS.