Задание 1

В архиве два письма. Письма содержат документы, ведущие на настоящие фишинговые сайты. Проанализируйте их. Ответьте на следующие вопросы

1. От кого эти письма?
2. На какой почтовый ящик будет отправлен ответ на эти письма?
3. Куда ведут ссылки? Что на этих ресурсах?
4. Что известно о доменах куда ведут ссылки?
5. Какой хэш вложенного документа?
6. Прошли ли письма SPF? Какой вердикт?
7. Было ли проверено вложение средством защиты? Какой вердикт?

Задание 2

Имитируем ситуацию. Три часа ночи. Вы находитесь в ночной дежурной смене. Приходит алерт, что на Windows ноутбуке секретаря обнаружен подозрительный excel документ. Ноутбук находится в офисе.

1. Какие ваши первичные действия?
2. Что будете смотреть из логов, чтобы убедиться, что файл действительно вредоносный?
3. Что будете делать с ноутбуком, с учетной записью? Каким образом?
4. Как будете доставать файл с ноутбука? Если вы используете инструменты, то опишите какие.
5. Как файл мог оказаться на хосте? Опишите всевозможные варианты
6. Будете ли вы связываться с пользователем? Каким способом и почему?
7. Для каждого способа из п.4 опишите какие методы сдерживания вы примените? Почему?
8. Для каждого способа из п.5 опишите какие индикаторы можно собрать? Где будете их искать?
9. Где можно заблокировать разные типы индикаторов из п.8?
10. Что известно об индикаторах excel документа?
11. Какие меры можно предпринять, чтобы в будущем защититься от таких атак?

Дополнительные вопросы:

12. Как можно найти и отозвать письма с Exchange сервера? Напишите PowerShell команду
13. Как проверить когда у пользователя менялся пароль? Напишите PowerShell команду