МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Тульский государственный университет»

Институт прикладной математики и компьютерных наук

Кафедра информационной безопасности

**Исследование угроз, связанных с электронной почтой**

отчёт по лабораторной работе №3

по курсу «Системы обнаружения вторжений»

Выполнили: студенты гр. 230781 \_\_\_\_\_\_\_\_\_ Глейм С.М.

(подпись)

\_\_\_\_\_\_\_\_\_ Ивлев А.Р.

(подпись)

Проверил: асс. каф. ИБ \_\_\_\_\_\_\_\_\_ Чаговец С.Н.

(подпись)

Тула, 2022 г.

**Лабораторная работа №3**

**Исследование угроз, связанных с электронной почтой**

**Цель работы**

Изучение и исследование угроз, связанных с электронной почтой.

**Задание на работу**

1. Подключиться с помощью телнет-клиента к указанному преподавателем тестовому серверу и отправить вручную или с помощью самостоятельно реализованного приложения тестовое письмо с произвольными полями отправителя. Как можно защитить почтовый сервер от такого типа писем?
2. Исследовать в виртуальной среде образец опасного сообщения электронной почты. По каким критериям его можно отнести к опасным? Определили ли антивирус тестовое вложение?

**Ход работы**

Для выполнения первого задания было выполнено подключение к указанному преподавателем SMTP-серверу с помощью telnet-клиента и вручную отправлено письмо с произвольными полями отправителя. Ход подключения и отправки представлен ниже на рисунке.

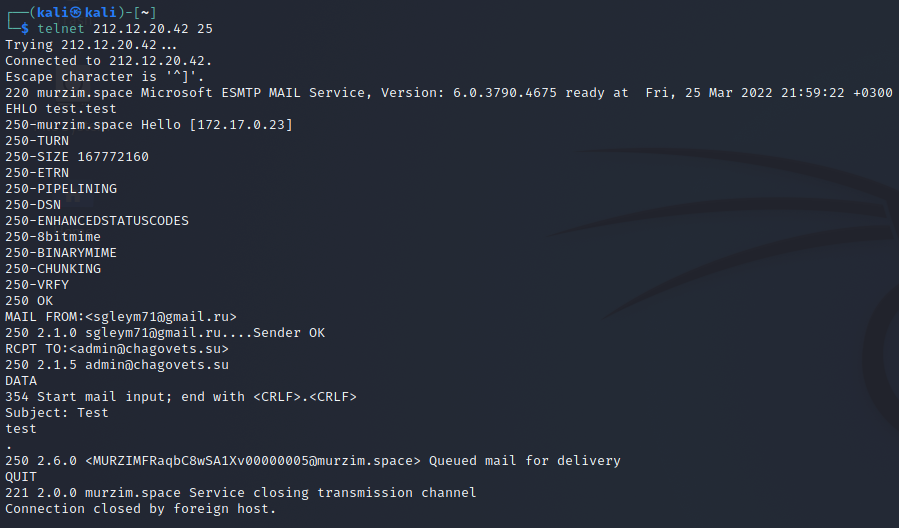


Рисунок 1 - Отправка сообщения с помощью telnet-клиента

Таким образом, протокол SMTP никак не защищает пользователя от сообщений различных адресатов с неизвестных доменов. Для предотвращения этого можно после получения домена отправителя отправлять запрос на IP-адрес подключенного клиента чтобы узнать истинное доменное имя и если два имени сходятся, то пропускать сообщение. Также можно настроить SMTP-сервер так, чтобы он выполнял пересылку только для пользователей своего домена, это также защитит от неизвестных источников писем.

Так как SMTP передает письма в открытом виде, значит SMTP-пакет можно перехватить и свободно прочитать. Для защиты от такого рода угроз стоит использовать обновленный протокол ESMTP, в котором возможна передача сообщений с применением TLS протокола.

Для выполнения следующего задания на виртуальной машине был установлен почтовый клиент Thunderbird и скачаны образцы опасных сообщений. К каждому сообщению было прикреплено вложение с вредоносными файлами. Все вложения скачивались в общую сетевую папку с основой машиной с установленным на ней антивирусом Kaspersky. Антивирус сразу же предупреждал о опасных файлах как уже распакованных архивов вложений, так и в не распакованных архивах. В каждом из трех образцов сообщений были найдены троянские программы.

Результаты обнаружения представлены ниже на картинках.

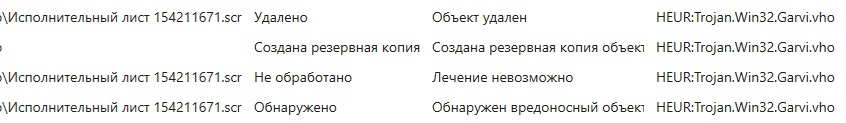


Рисунок 2 - Предупреждение антивируса о вредоносной программе (письмо №1)

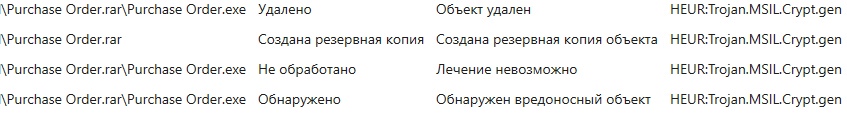


Рисунок 3 - Найденный в архиве вредоносный файл (письмо №2)

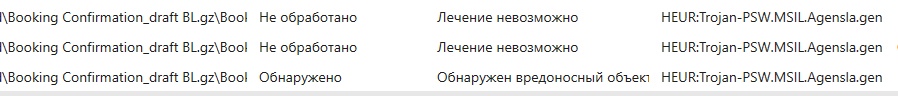


Рисунок 4 - Зараженный архив (письмо №3)

**Вывод**

Нами были изучены и исследованы угрозы, связанные с электронной почтой.

Протокол SMTP не обладает никакими механизмами защиты как от спама, так и от прослушивания. Для обеспечения безопасности стоит использовать протокол ESMTP и проверять домен отправителя.

Для защиты от опасных писем необходимо иметь регулярно обновляемое антивирусное ПО и открывать вложения в безопасных средах (например, песочницах или виртуальных машинах).