



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДФУ)

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра информационной безопасности

Лабораторная работа №2

Выполнили студенты гр. М9120-
09.04.02ИБКФС

Ефременко И.В.,
Медведев Н.В

Старший преподаватель

С.С. Зотов

зачтено / не зачтено

г. Владивосток
2022

The image shows a Kali Linux desktop environment. On the left is a vertical sidebar with icons for Trash, File System, Home, and a folder named 'bolt' (with a Russian label 'bolt'оманды). The main area is divided into two windows. The left window is a terminal titled 'root@kali: /home/kali/Downloads/gophish-v0.11.0-linux-64bit'. It shows the execution of 'sudo su', 'password for kali:', 'chmod +x gophish', and the running of 'gophish'. The output shows the application starting, migrating the database, and displaying a list of configuration files. The right window is a file manager titled 'gophish' showing the contents of the 'gophish-v0.11.0-linux-64bit' directory. It contains folders like 'db', 'static', 'templates', and files like 'nfig.json', 'gophish', 'gophish.db', 'ih_admin.crt', 'gophish_admin.key', 'LICENSE', 'ADME.md', and 'VERSION'. The desktop background is dark with a grid of icons for various applications and system utilities.

Сервис заработал и мы попали на главную страницу localhost.

The screenshot shows the Gophish web application running in a browser. The browser's address bar displays the URL `https://127.0.0.1:3333`. The Gophish logo is visible in the top left corner of the application. The top navigation bar contains the following links: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management (with an Admin button), and Webhooks (with an Admin button). The main content area features the word "Dashboard" in a large, bold font, followed by a light blue message box that reads: "No campaigns created yet. Let's create one!".

Произвели покупку домена:

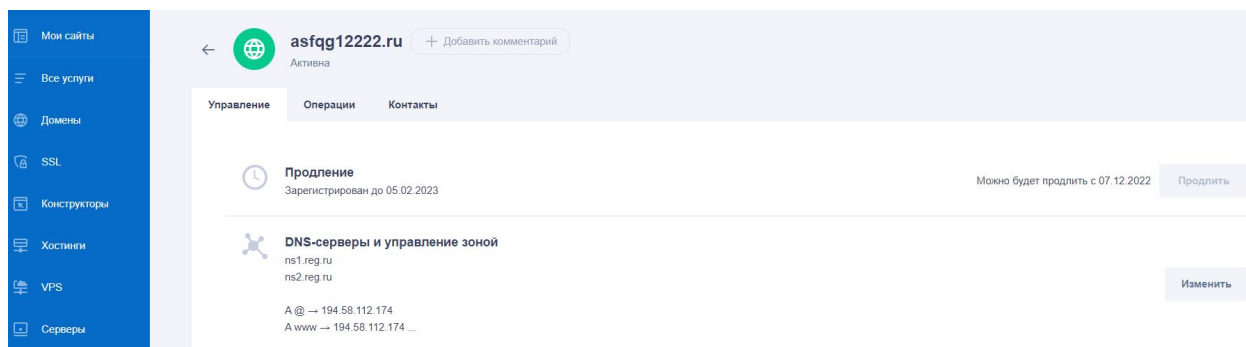


Рисунок 3 Домен на REG.ru

После создали письмо с, прилагающемся к нему, файлу. Содержание данного письма представляет собой обычное приглашение на ИТ мероприятие.

Уважаемые студенты,

Уведомляем вас о том, что ФГБОУ ВО «Уральский государственный педагогический университет» при поддержке ФГАУ «Ресурсный молодежный центр», АНО «Россия — страна возможностей». Министерства образования и молодежной политики Свердловской области реализует проект «Всероссийский педагогический хакатон «HackEducation 2.0».

HackEducation 2.0 - педагогический хакатон для IT-разработчиков и педагогов в возрасте от 18 до 30 лет. Направлен на формирования условий взаимодействия для решения актуальных проблем и задач модернизации системы отечественного образования.

Хакатон представляет собой соревнование объединенных студенческих команд и включает в себя 2 этапа, в рамках которых необходимо представить собственную технологическую идею образовательного цифрового продукта, а также разработать прототип на основе идеи и презентовать его на публичной защите. Команды примут участие в лекциях от экспертов, менторских сессиях, партнерских активностях и мероприятиях.

В прикрепленный файлах вы можете ознакомиться с положением и памяткой для участников.

Более подробная информация по ссылке - <https://vk.com/hackeducation>

Рисунок 4 Текст письма

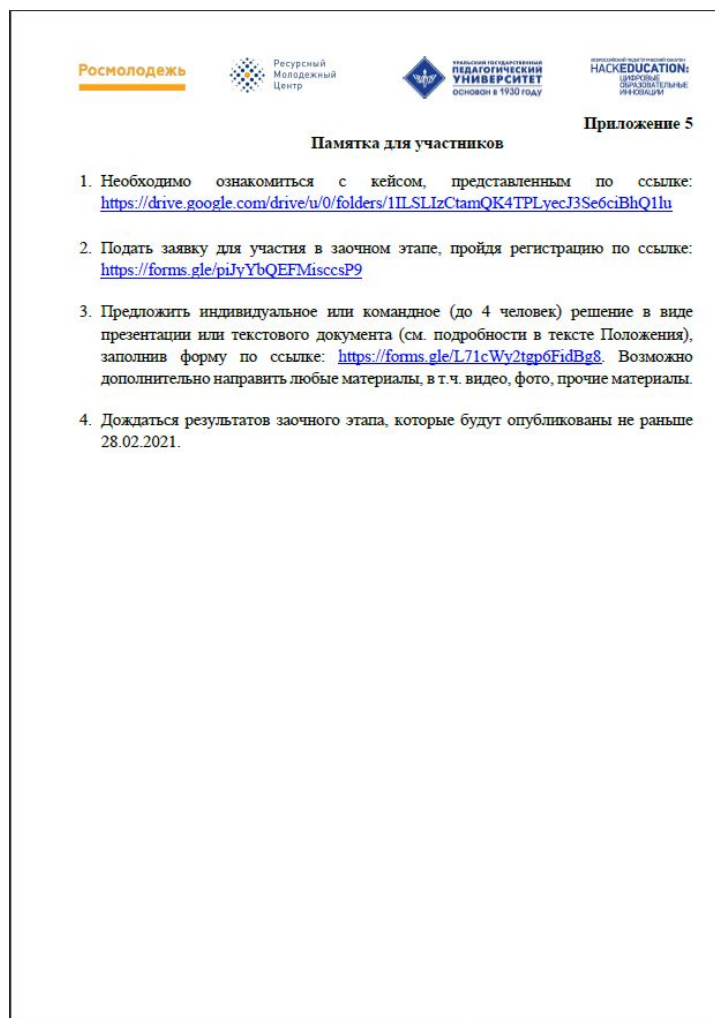


Рисунок 5 Файл в закрепе

Данный файл необходимо было сконвертировать через canarytoken, создав тем самым скрипт, который отошлёт нам информацию о запущенной системе. Конвертирование показано на рис 6., а его срабатывание на рис. 11.

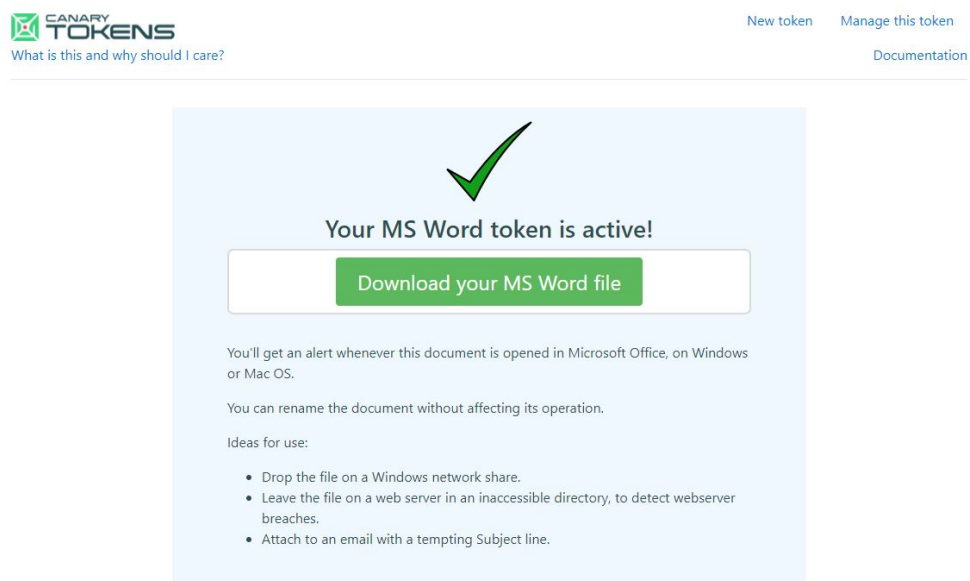


Рисунок 6 Создание токена

Далее была произведена настройка отправителя и сообщения в gobhish, после чего предприняли попытку выслать тестовый email.

The screenshot shows the 'New Sending Profile' configuration page. It includes fields for Name (Наездников Максим), Interface Type (SMTP), From (Наездников Максим <Hakaton_IT@dvfu.ru>), Host (smtp.yandex.ru:585), Username (hyt), and Password (masked with dots). There is a checkbox for 'Ignore Certificate Errors' which is checked. Below these are 'Email Headers' with a table containing 'X-Custom-Header' and '{{URL}}-gophish'. A '+ Add Custom Header' button is also present. At the bottom, there is a table with columns 'Header' and 'Value' and a message 'No data available in table'.

Рисунок 7 Отправитель

The screenshot shows the 'Import Email' configuration page. It includes a red 'Import Email' button at the top. Below it is a 'Subject' field with the text 'Общая информация для всех студентов'. There are tabs for 'Text' and 'HTML', with 'HTML' selected. The HTML content area contains Russian text about a digital product idea and a link to a VK page. Below the text area is a checkbox for 'Add Tracking Image' which is unchecked. There is a red '+ Add Files' button. At the bottom, there is a table with columns 'Name' and a file named 'Pamyatka_dlya_uchastnikov_Khakaton.pdf'. A pagination bar at the bottom shows 'Showing 1 to 1 of 1 entries' and 'Previous 1 Next'.

Рисунок 8 Сообщение

Данное сообщение пришло, но сразу же улетело в спам.

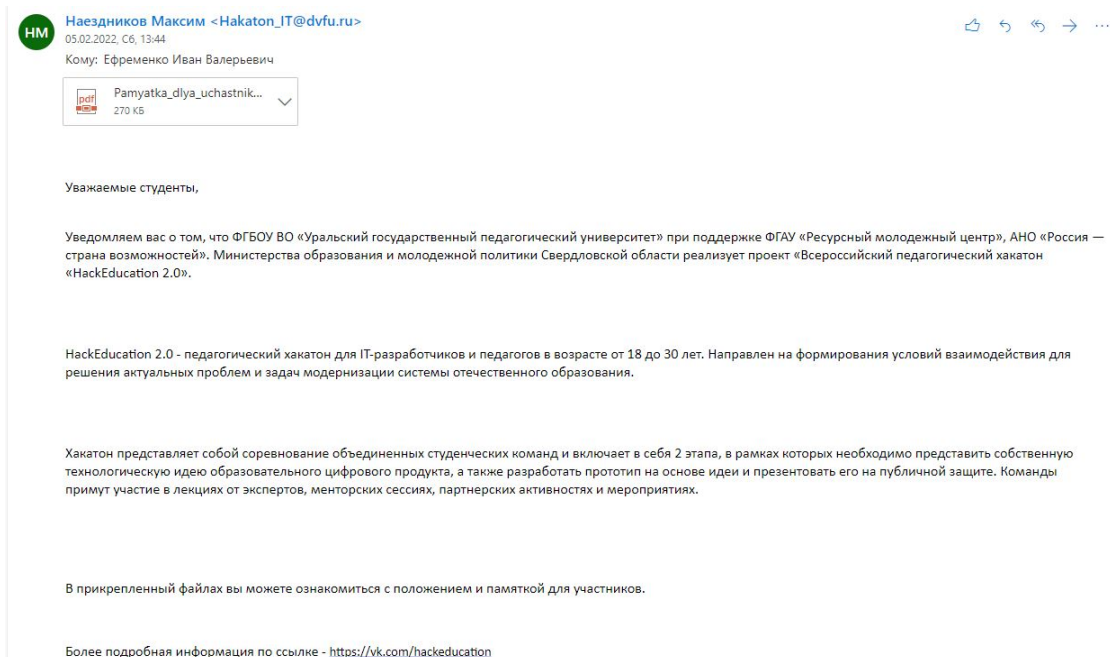


Рисунок 9 Сообщение

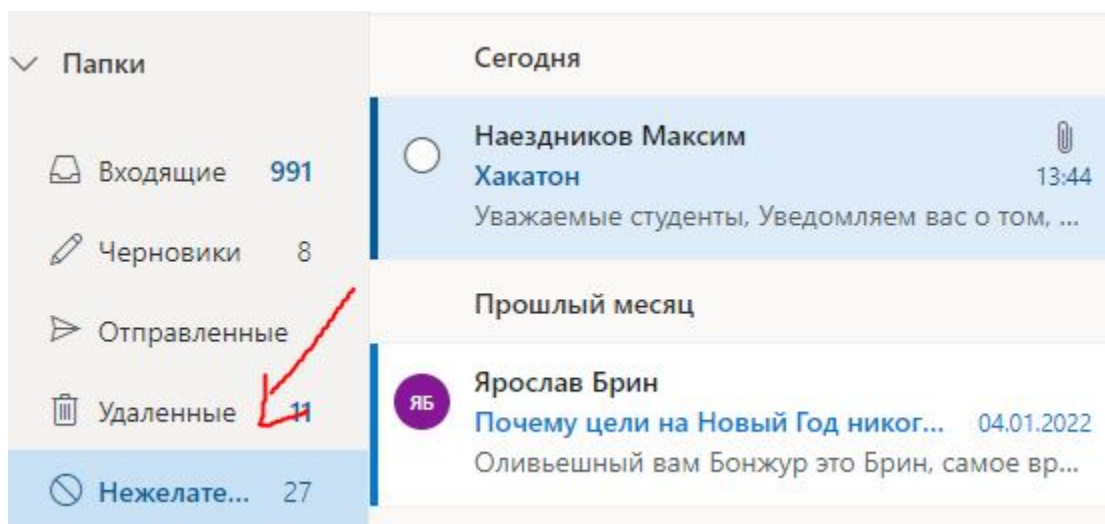


Рисунок 10 Спам

При открытии файла, срабатывает триггер, созданный на canarytoken.

Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 109.126.4.112.

Basic Details:

Channel	HTTP
Time	2022-02-05 03:35:59 (UTC)
Canarytoken	kkhvm3860ln1e18cv6b69cws1
Token Reminder	C:\Users\Nolling\Desktop
Token Type	ms_word
Source IP	109.126.4.112
User Agent	Mozilla/4.0 (compatible; ms-office; MSOffice 16)

Canarytoken Management Details:

Manage this Canarytoken [here](#)

More info on this token [here](#)

Powered by: [Thinkst Canary](#)

Рисунок 11 Его срабатывание