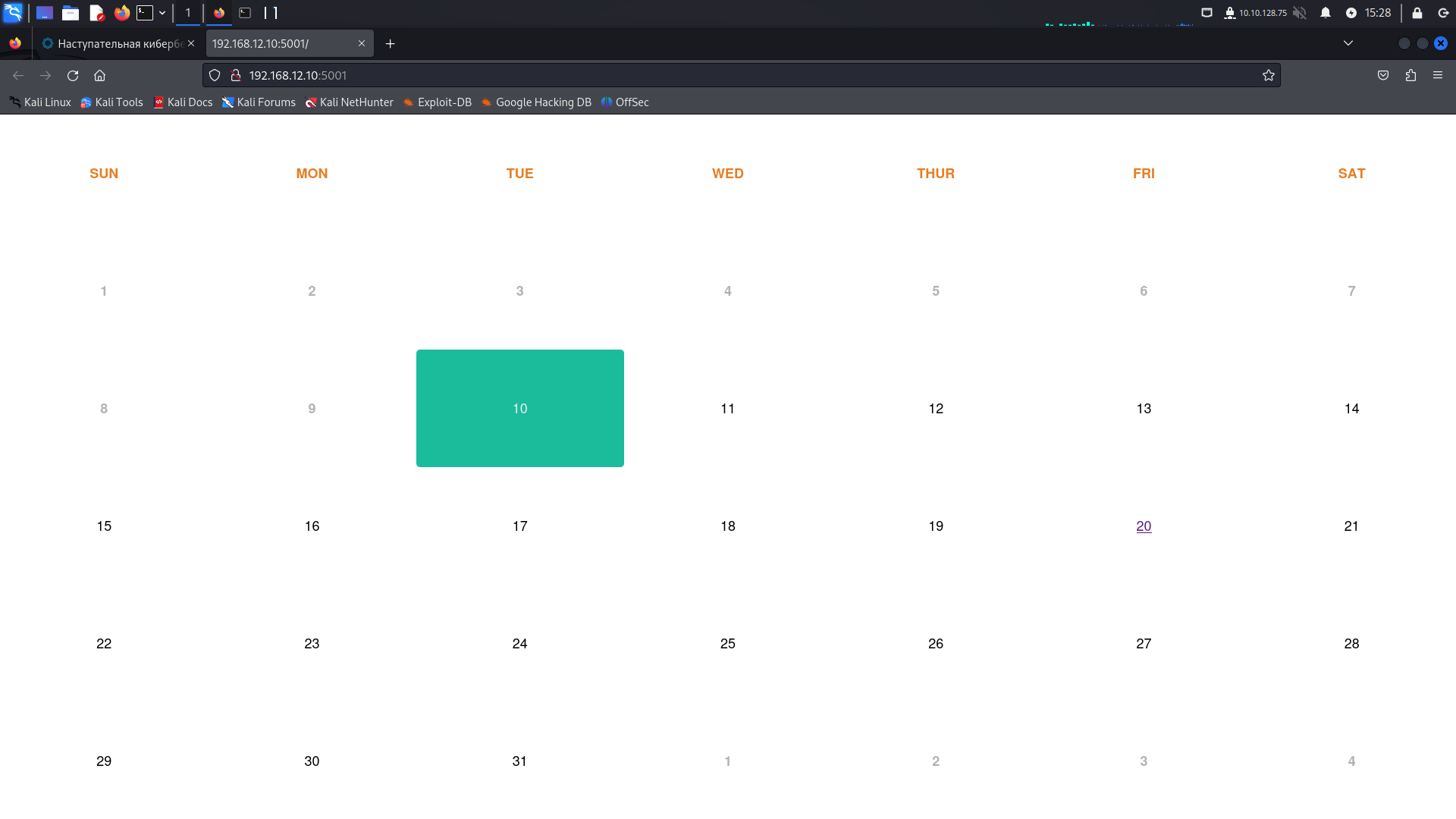
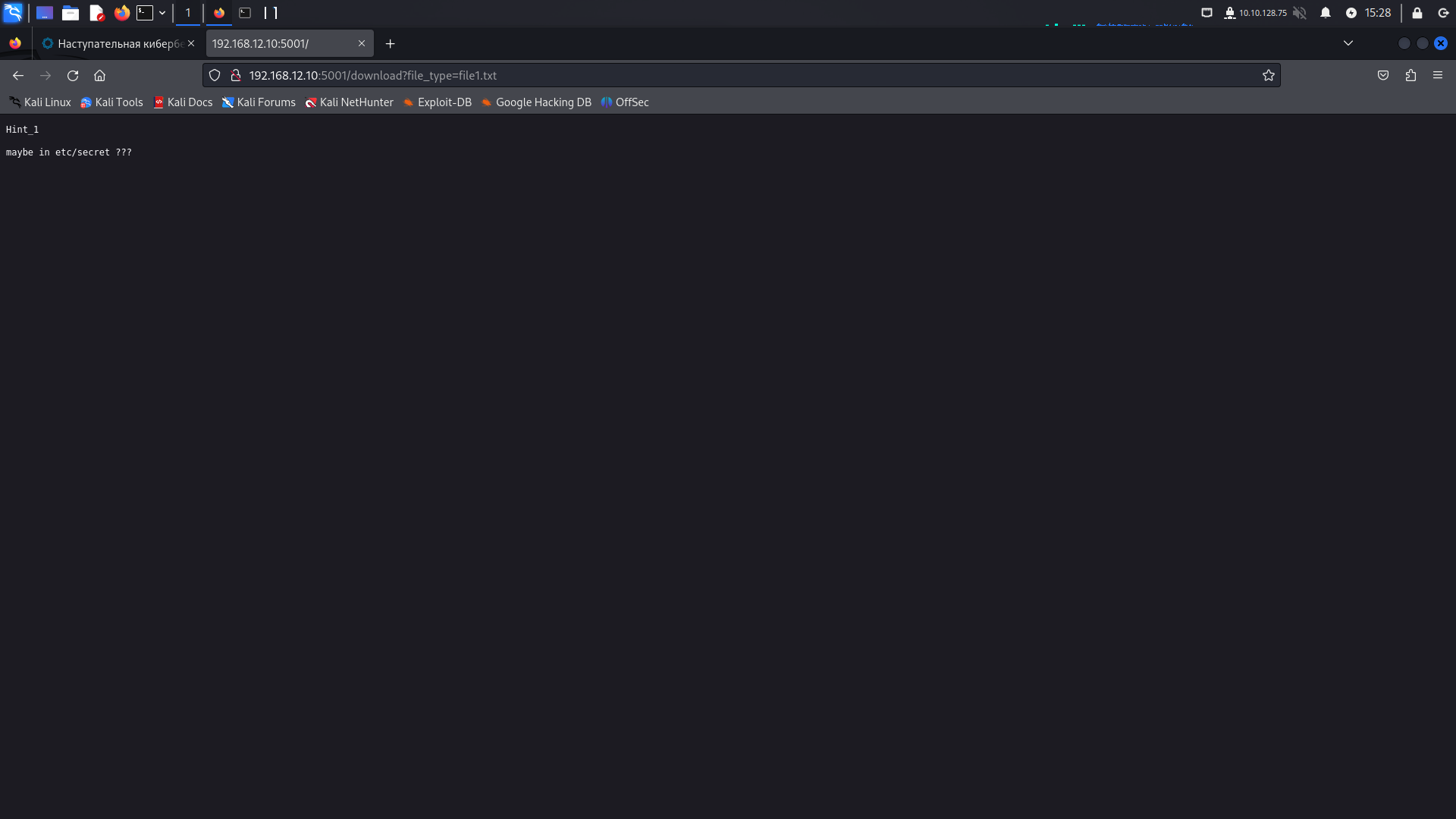
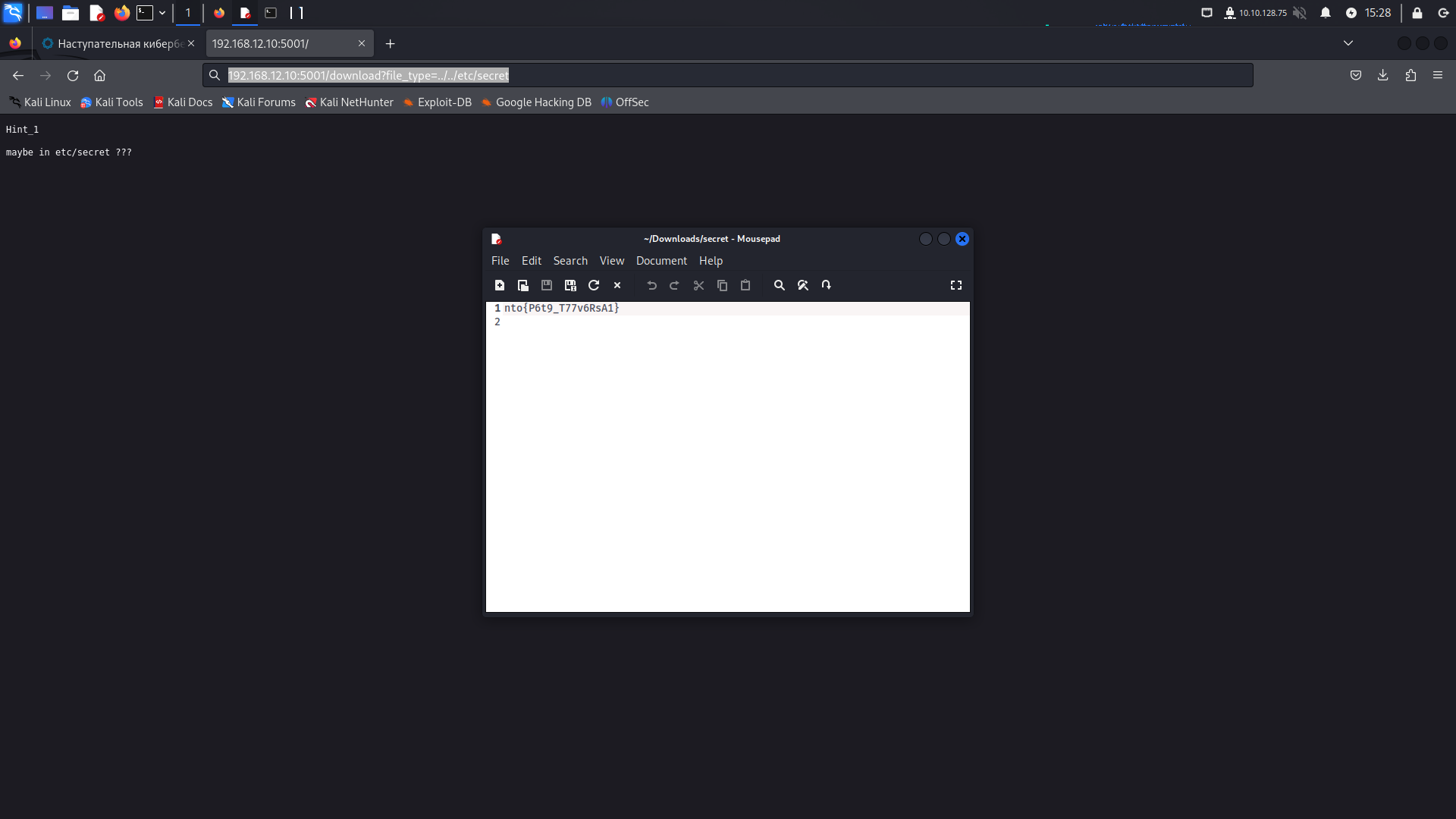
**CTF – Predictor**

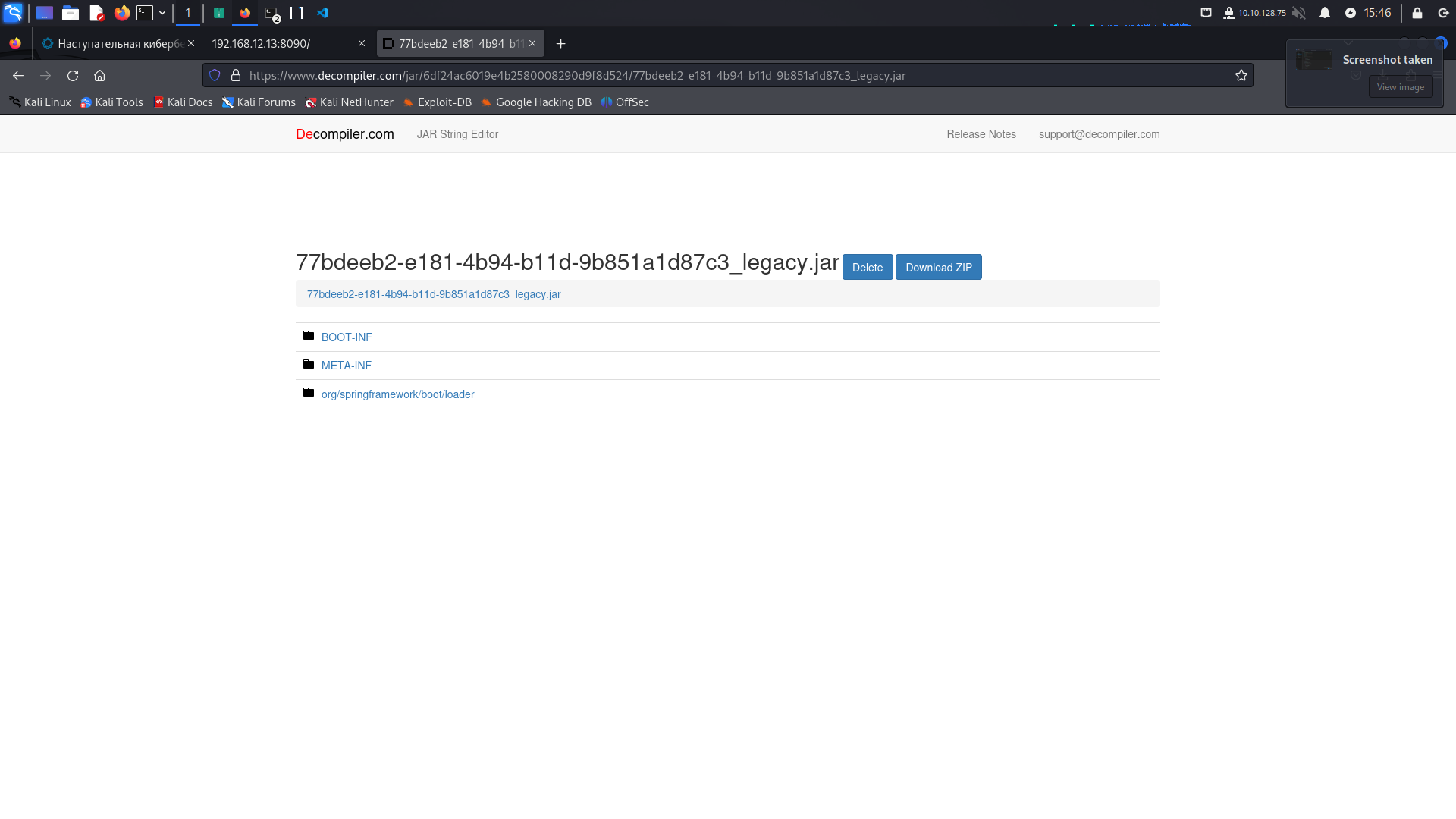
**Наступательная кибербезопасность**

WEB1: При переходе по ссылке, нас встречает календарь, где в 20 числе имеется ссылка на другую страницу

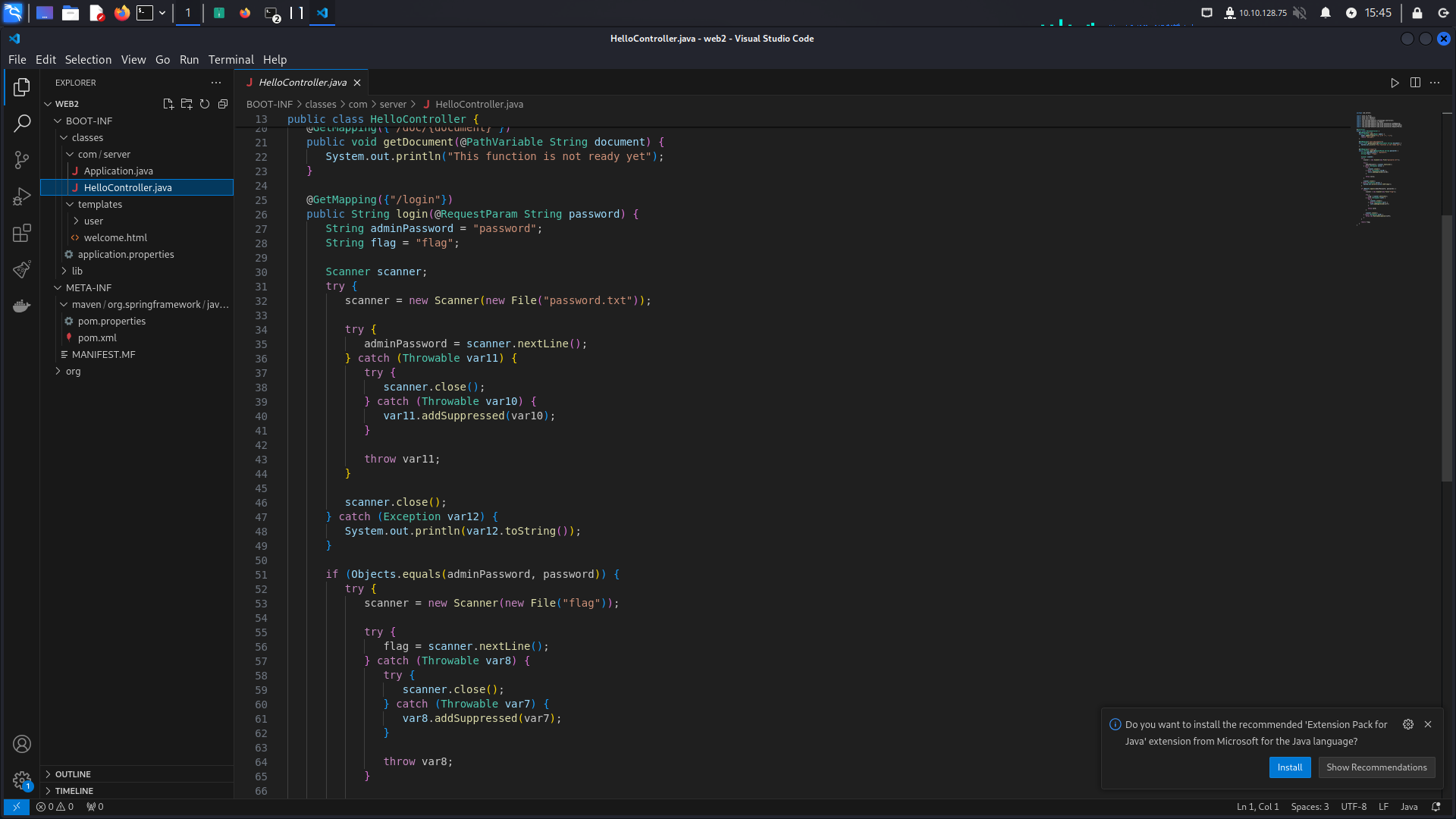
Переходя по ней, видно подсказку

Отсюда можно понять, что нужно перейти в корневой каталог и перейти к /etc/secret. Вбив адрес, скачивается файл с флагом

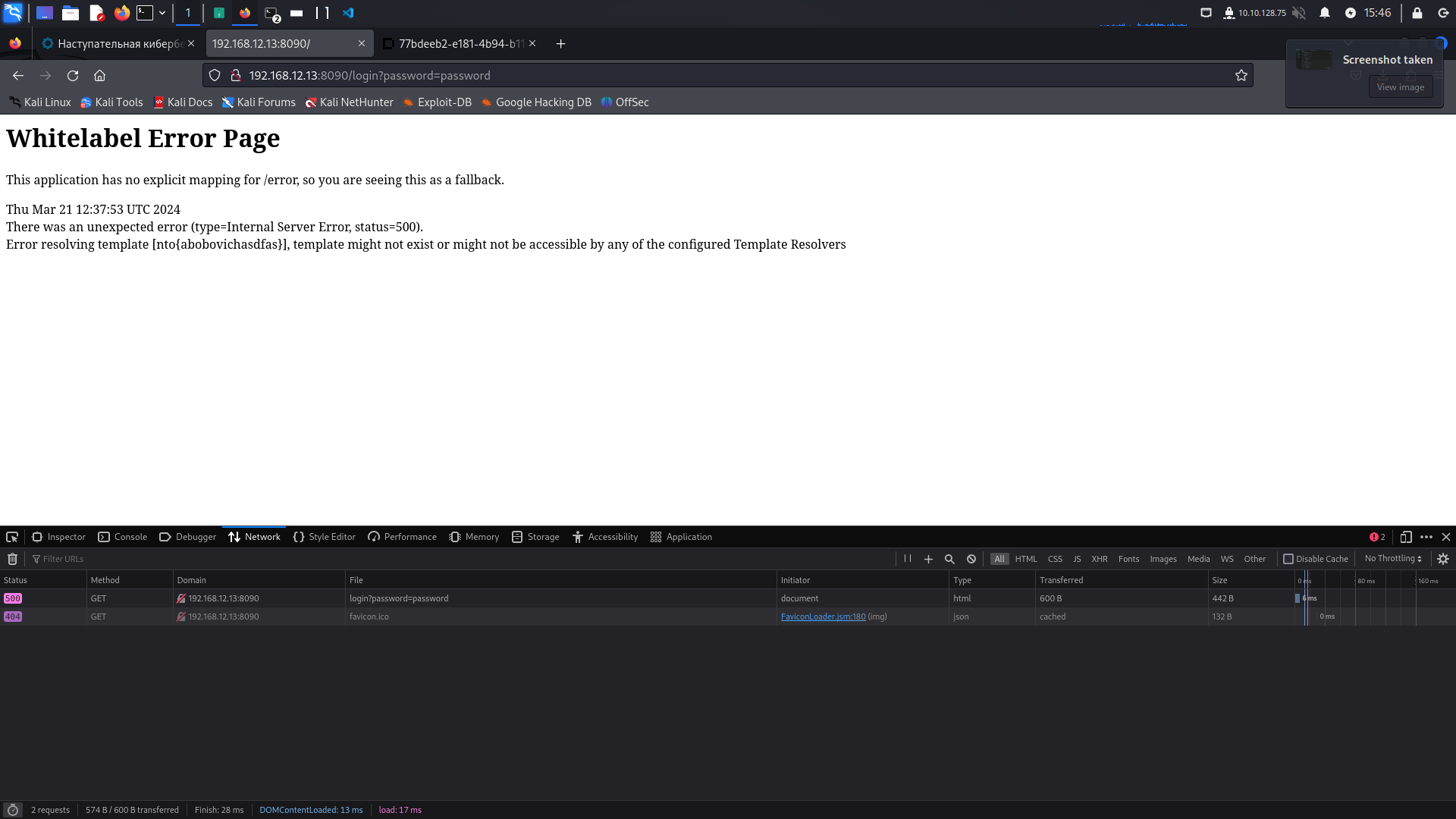
WEB2: Декомпилируем файл legacy.jar через онлайн декомпилятор



Откроем проект и нас интересует только файл BOOT-INF/classes/com/server/Application.java.

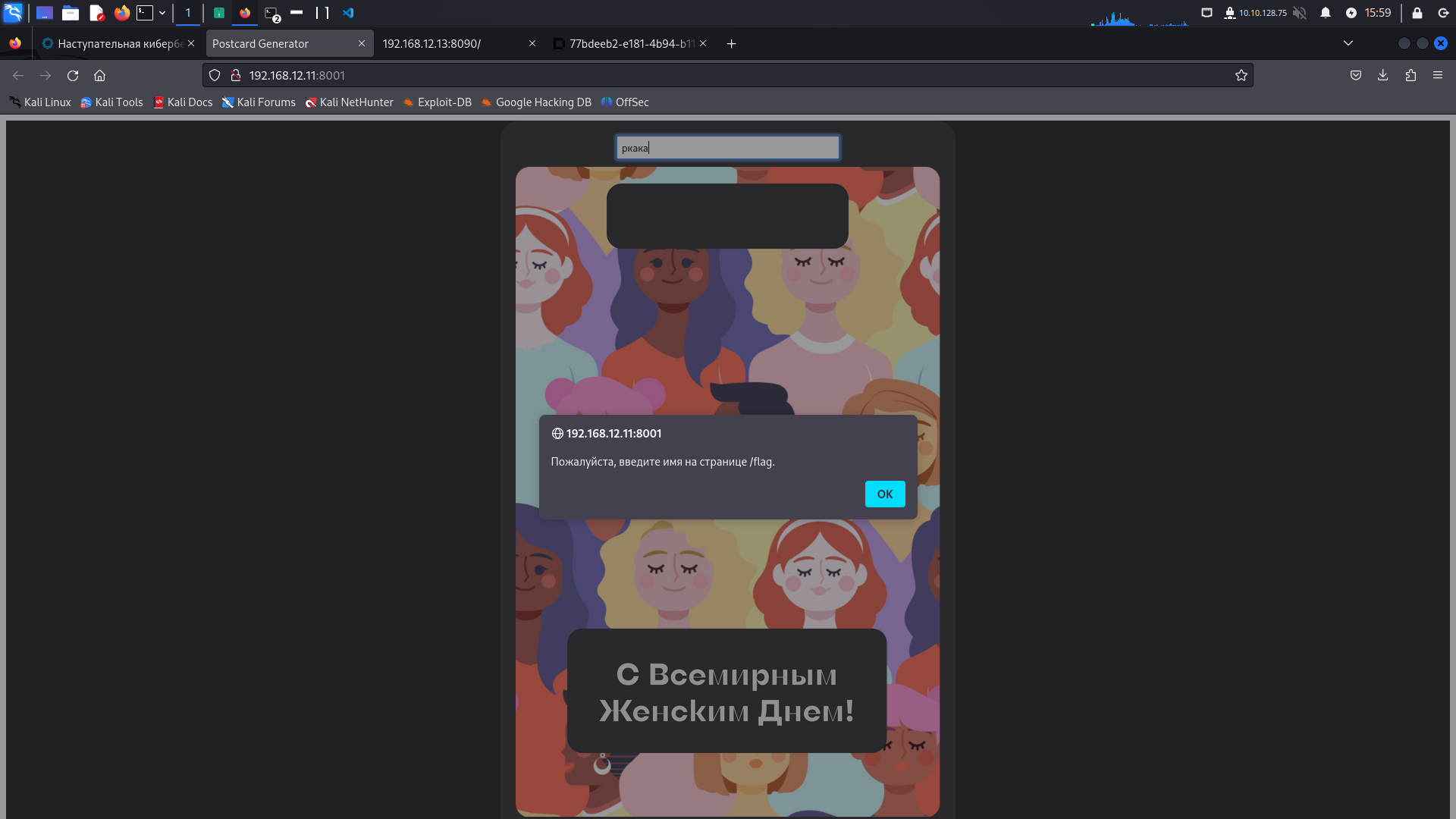
Здесь нужно указать параметр password и для получения флага, необходимо,

чтоб он был равен значению adminPassword=”password”. Указываем адрес <http://192.168.12.13:8090/login?password=password> и получаем наш флаг

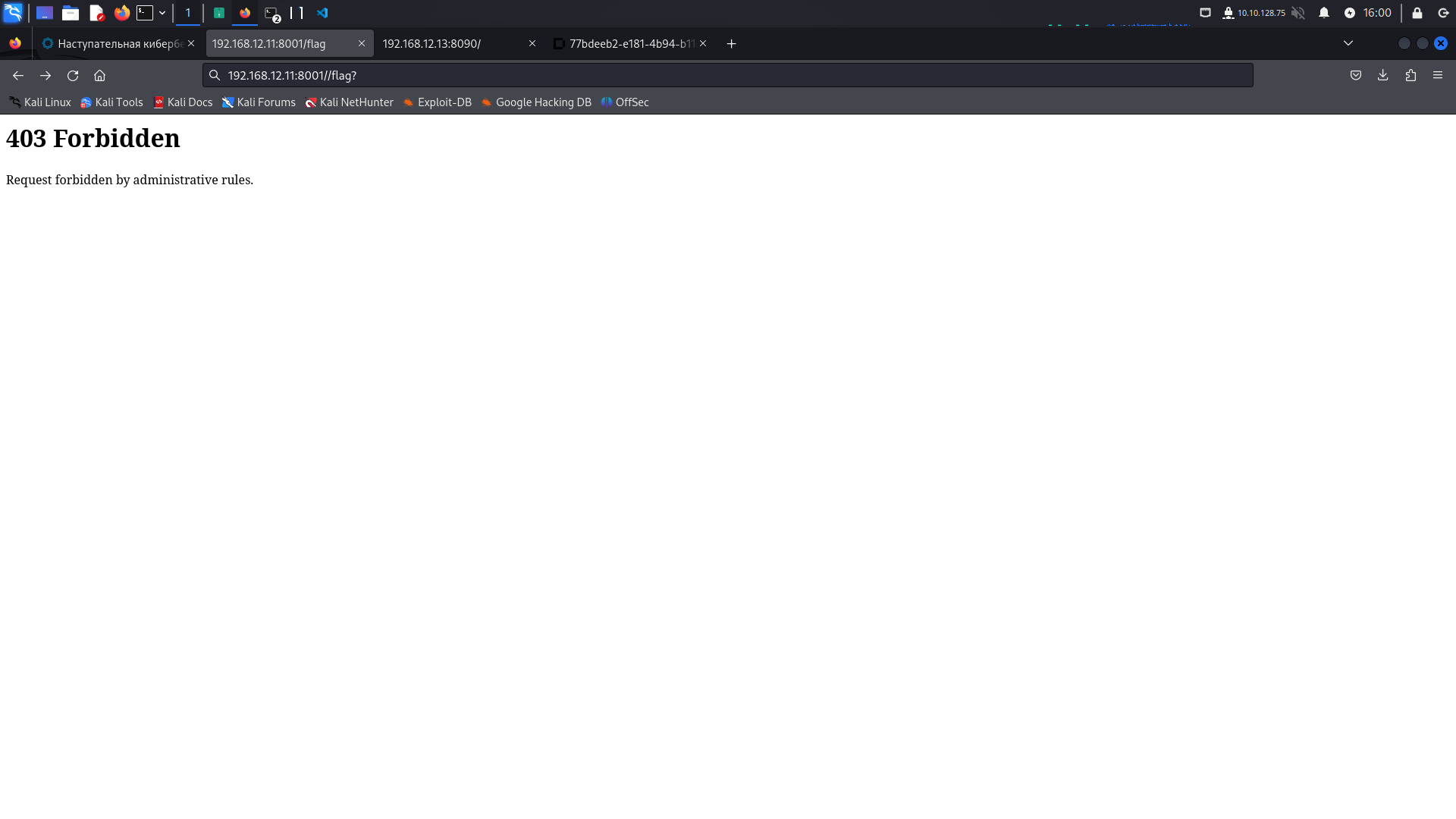


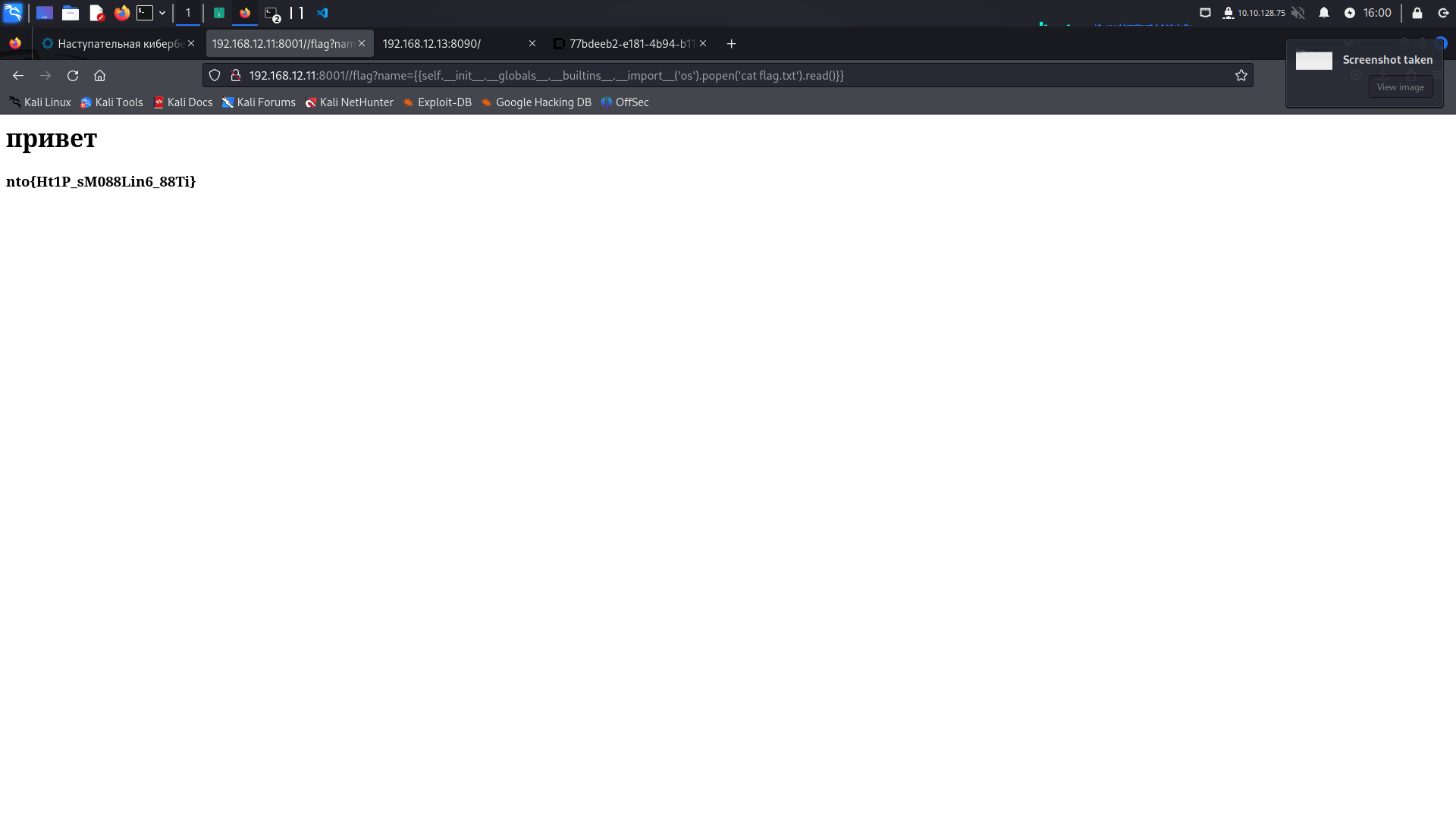
WEB3: Анализируем код файла app.py. Отсюда узнаем только о главной странице и странице /flag.

Откроем страницу:

При вводе любого значения просят перейти на страницу /flag. Там нас встречает

ошибка 403.

Обойти это можно с помощью **path fuzzing. С учетом того, что приложение написано на jinja и неправильно фильтруются знаки {{ и }}, то можно выполнить произвольный код через запрос.**

Прочитав файл flag.txt, получаем флаг

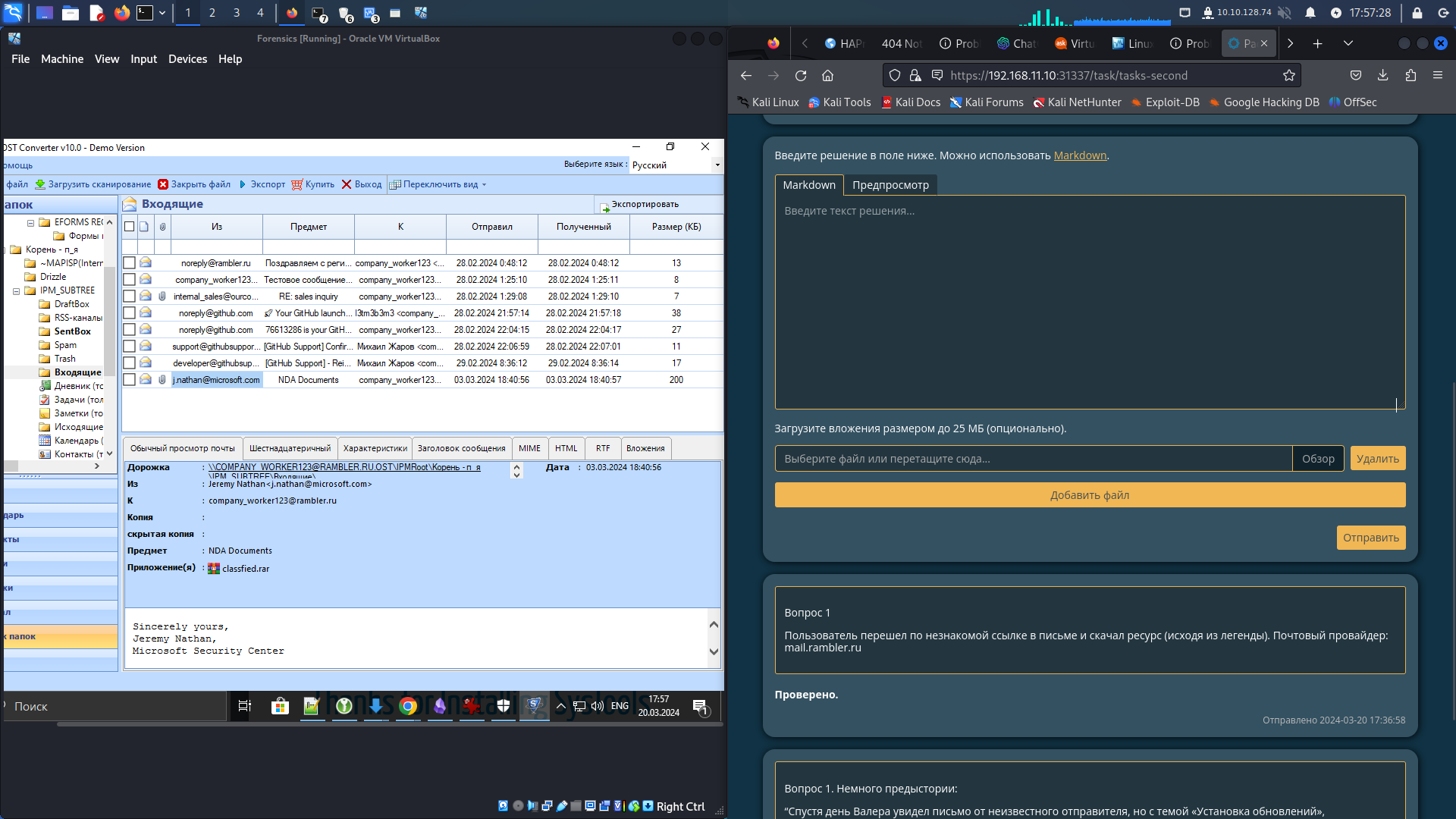
**Расследование инцидента**:

Вопрос 1

1. Исследовали файловую систему. (по запросу почты найденной в автозополнении браузера)
2. Нашли .ost
3. Разархивировали через онлайн сервис.
4. Нашли письмо с необычным содержанием.

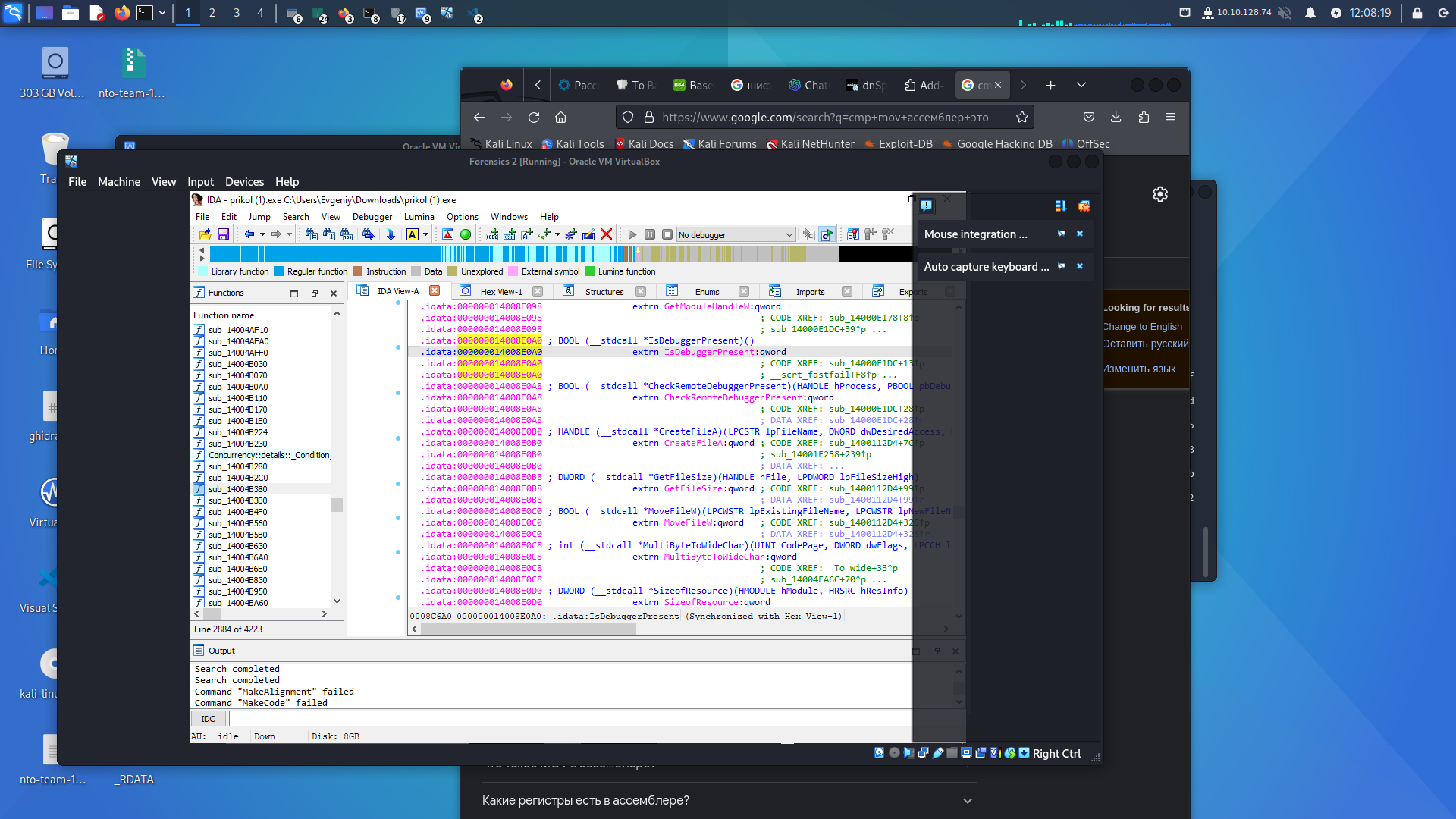
Вопрос 2 Почтовый провайдер рамблер.

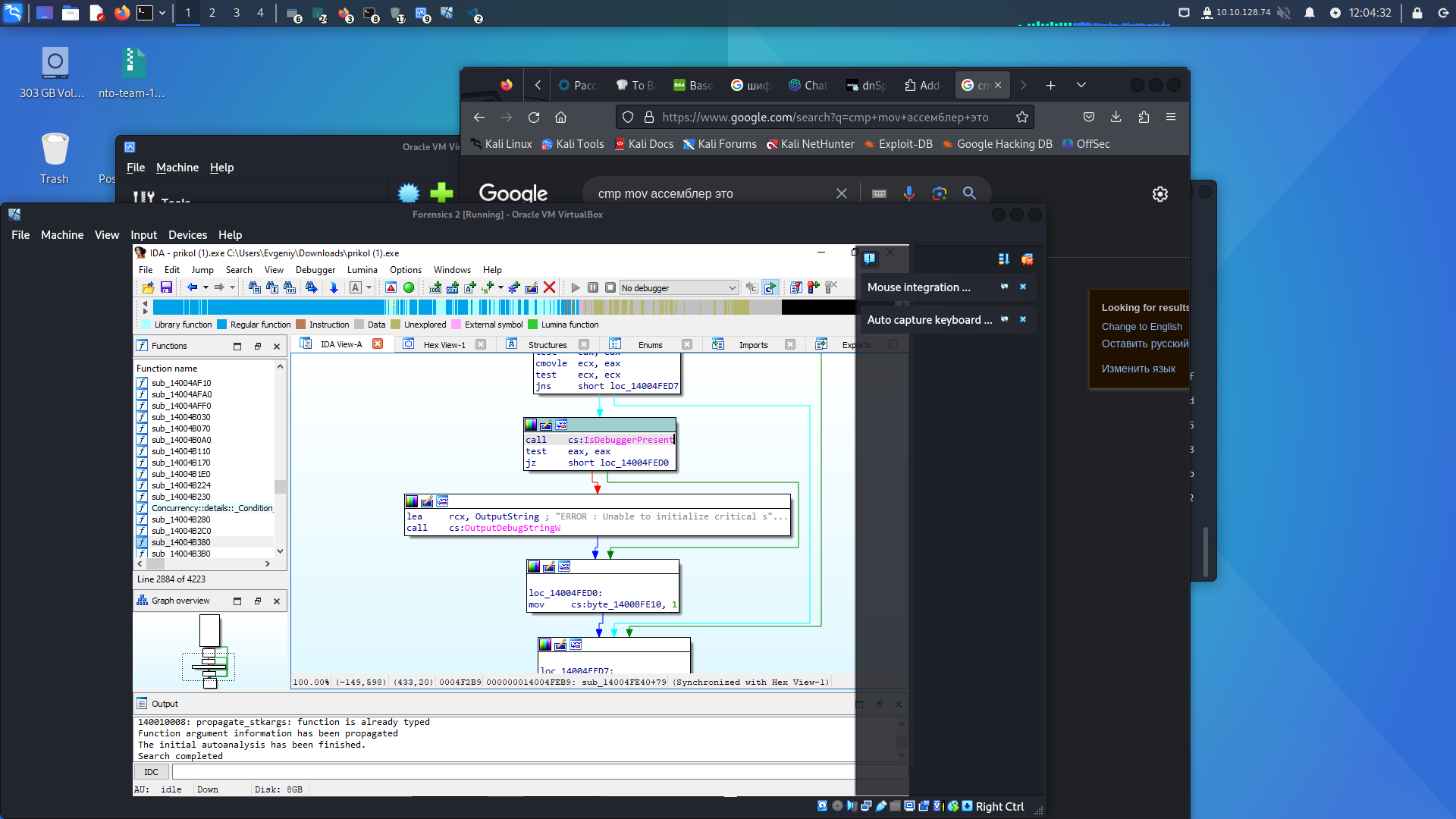
Вопрос 3

1. В прикрепленом архиве есть файл TOP\_SECRET.pdf.cmd (в виндовсе .cmd запускает скрипт в консоли). Название уязвимости: дроппер

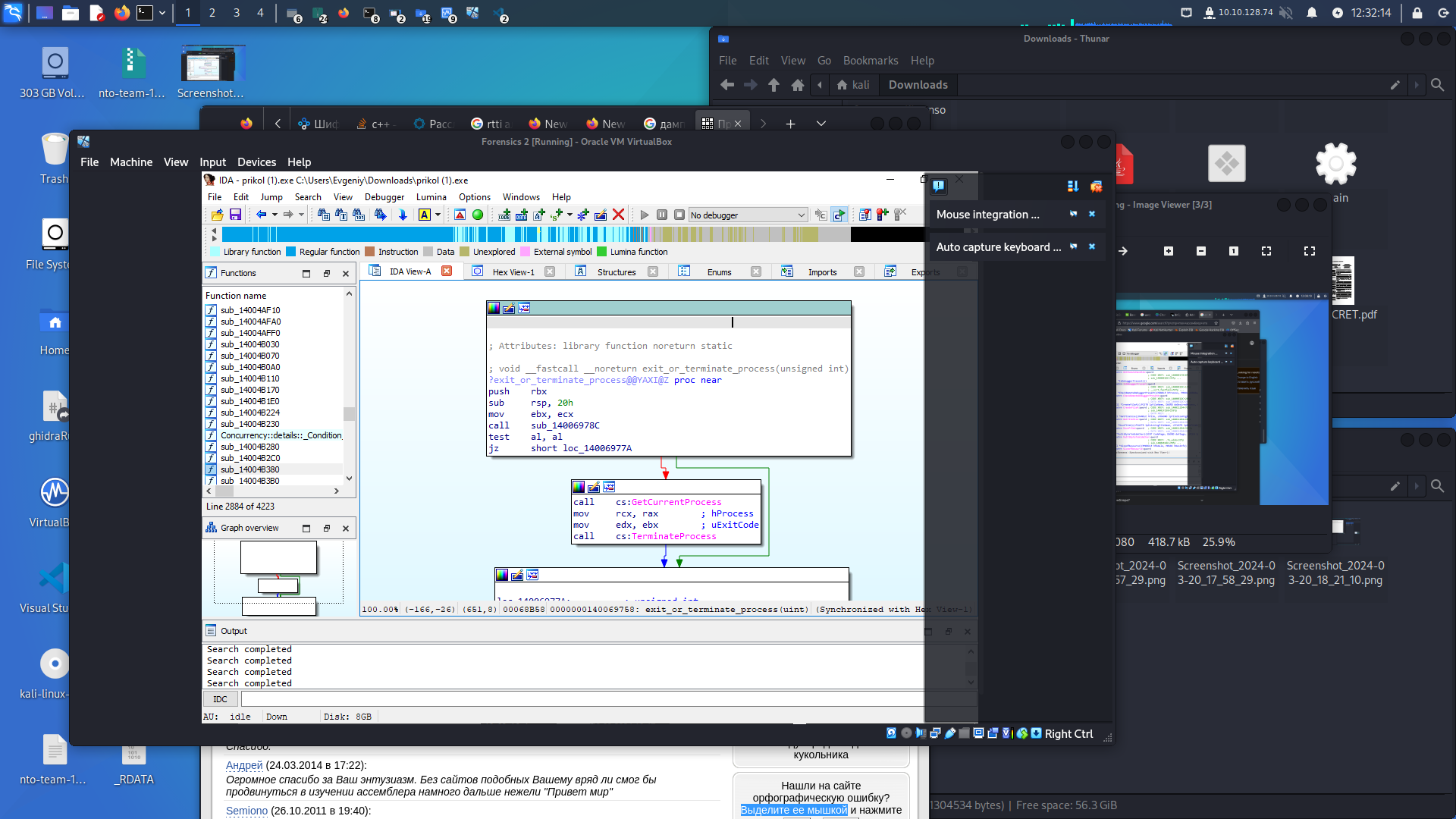
Вопрос 4

Программа отключает дебаггер. Прогнав через IDA файл prikol.exe(см вопрос 2), в котором находится вирус, мы нашли строки в которых указаны методы IsDebuggerPresent и CheckRemoteDebuggerPresent.





Также в prikol.exe содержатся строки с методами GetCurrentProccess и TerminateProccess, которые не дают открыть диспетчер задач и дебаггер



Вопрос 5

Алгоритм шифрования: CBC (Симетричное блочное шифрование). Шифруется при помощи библиотеки Crypto++

