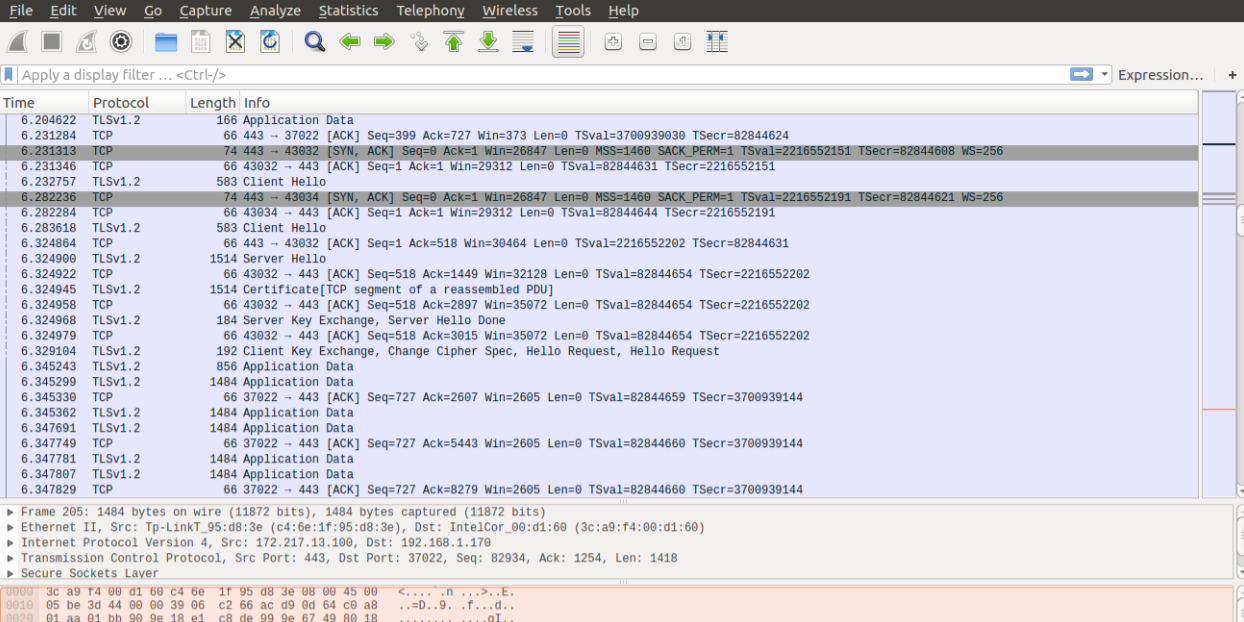
**19.6 Практика**

Устанавливаю Wireshark sudo apt install wireshark



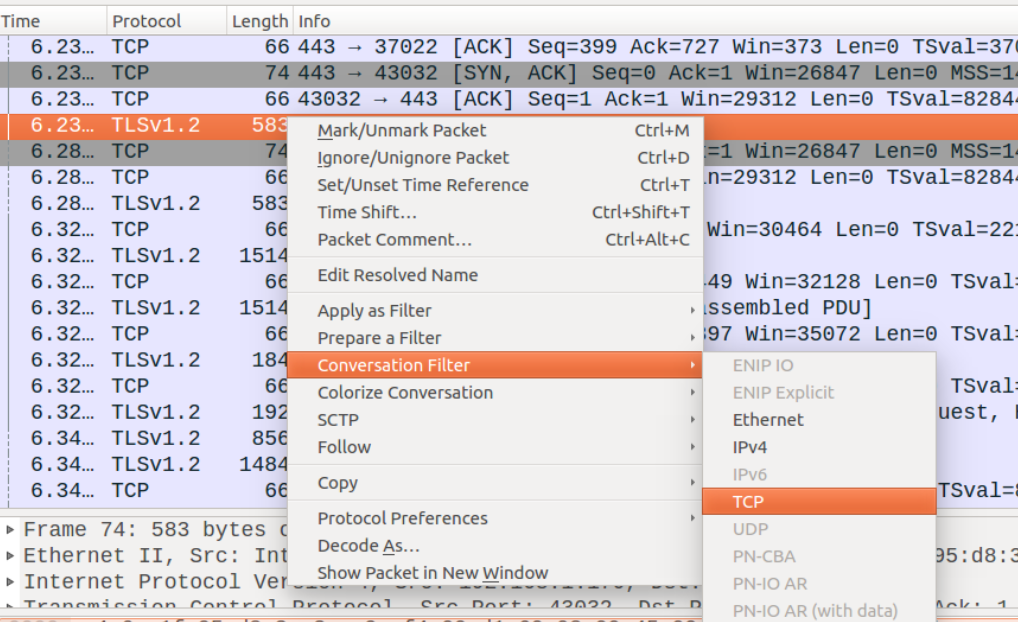
Сделаю захват пакетов

sudo tcpdump port 443 -w output.pcap

Открою pcap-файла с помощью Wireshark (wireshark output.pcap

Проверю “странное” TCP-соединение,

щёлкнув правой кнопкой мыши по интересующему вас пакету и выбрав в контекстном меню команду Conversation filter > TCP

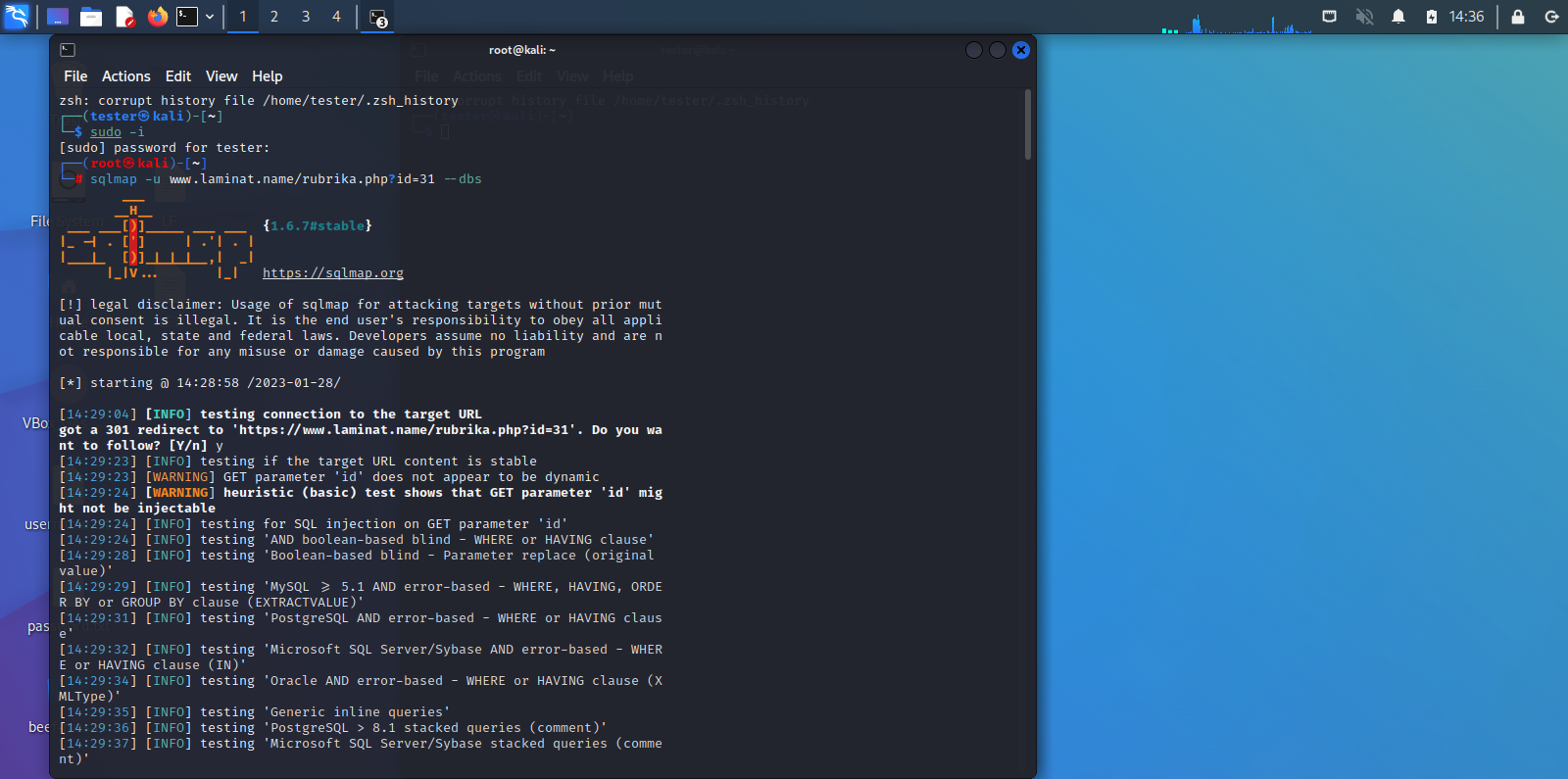


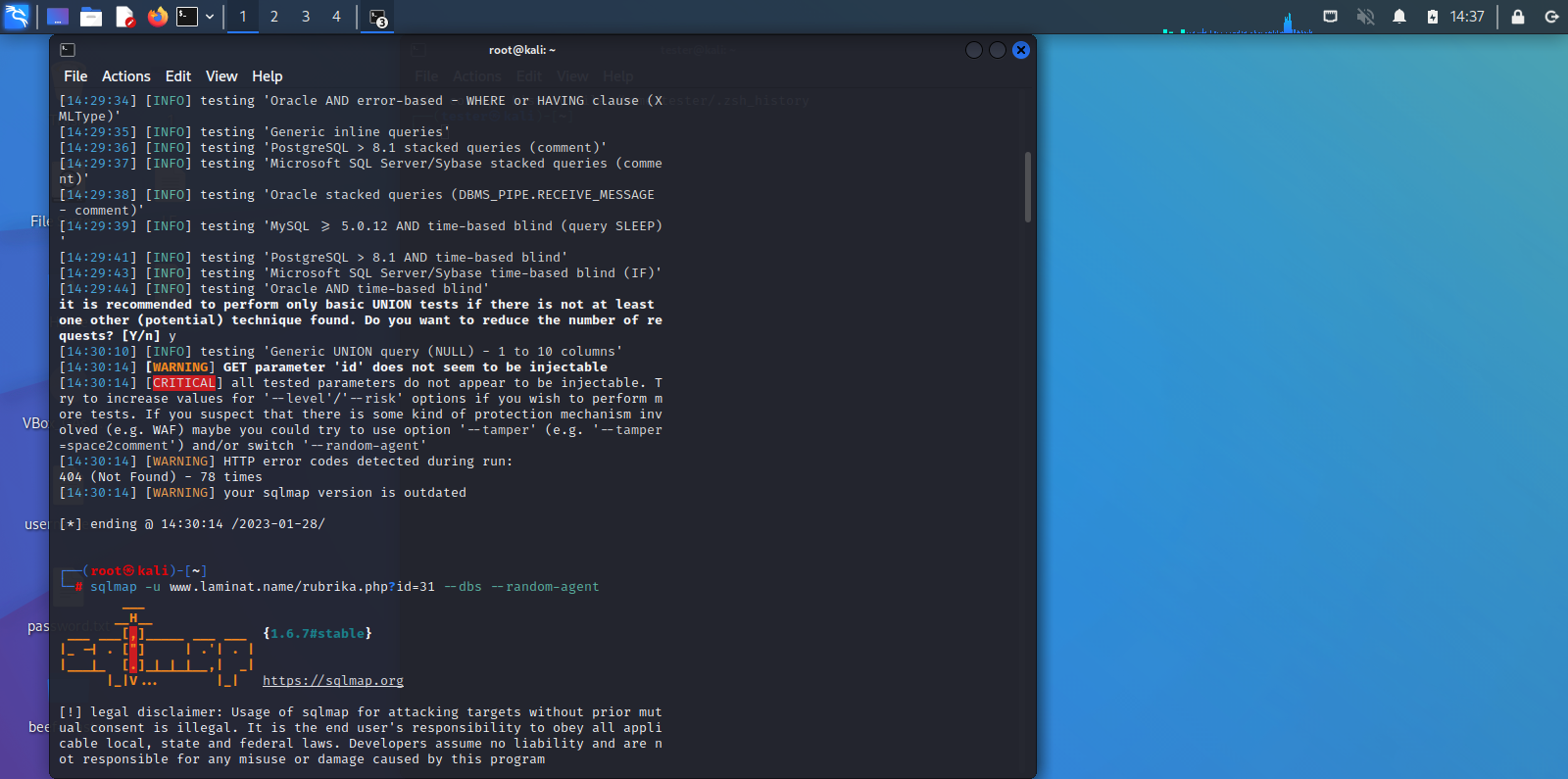
В соединении участвуют клиент и сервер, и что-то идёт не так либо на клиенте, либо на сервере. Это можно проверить, например, после отправки пакета client hello, если клиент отправит пакет FIN ACK, который завершал TLS-соединение, то означает, что соединение завершает клиент, а не сервер.

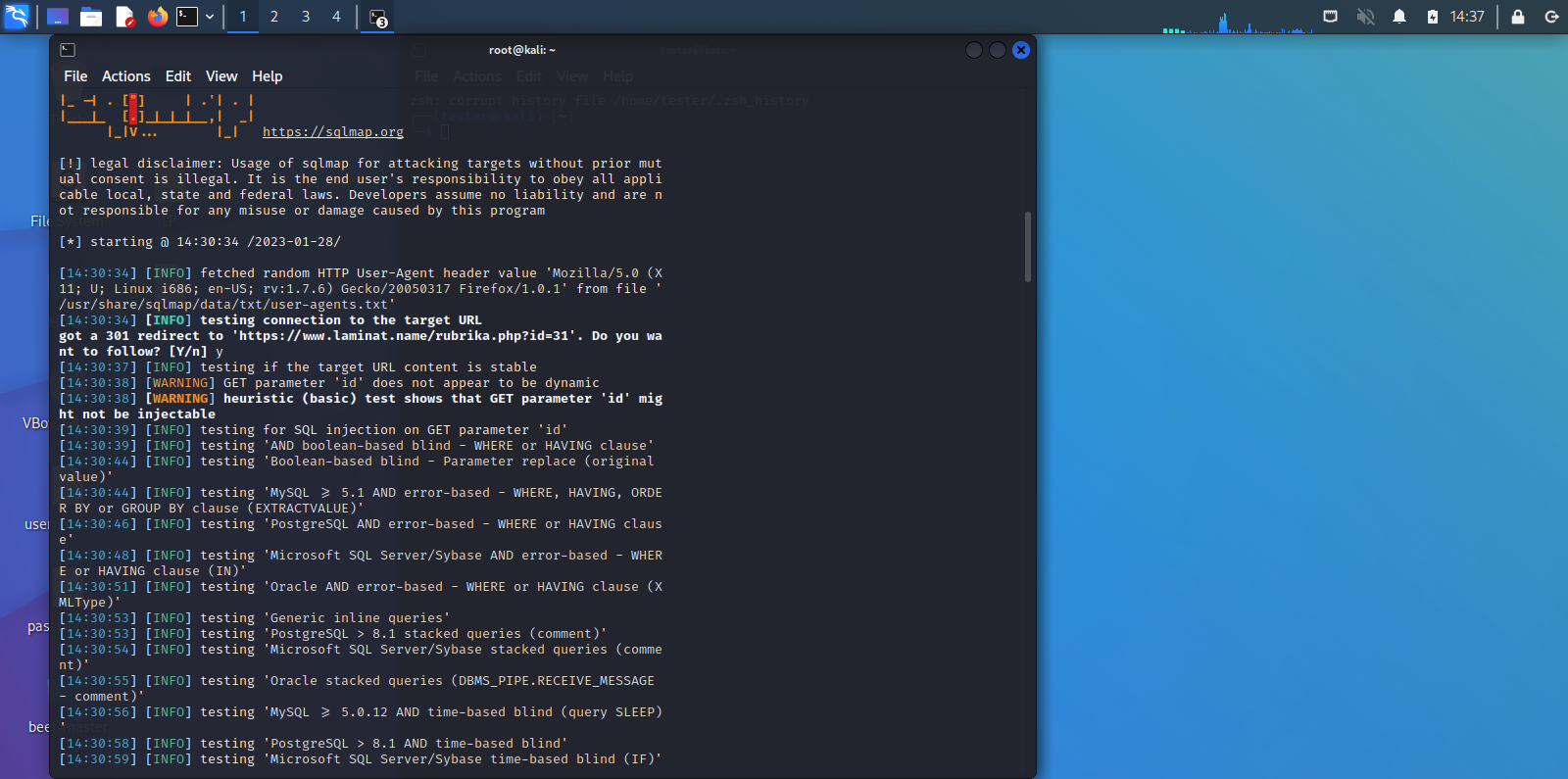
**SQLMAP**

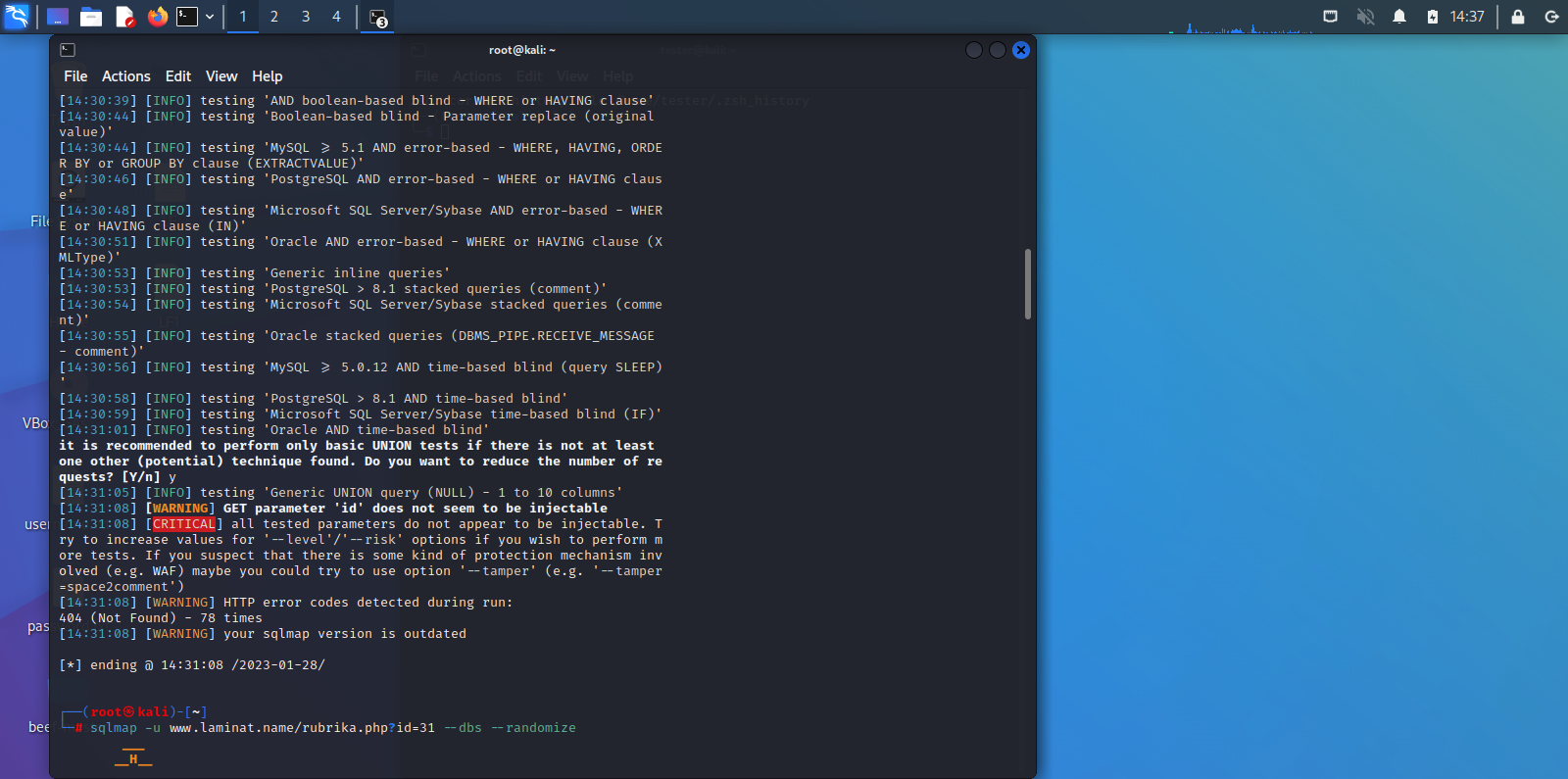
**Запустить утилиту sqlmap с целью осуществления атаки *SQL*-инъекции. Чтобы изучить работу sqlmap, предлагаю изменить и использовать следующие ключи (в дополнение к тем, которые необходимы для выполнения успешной атаки):**

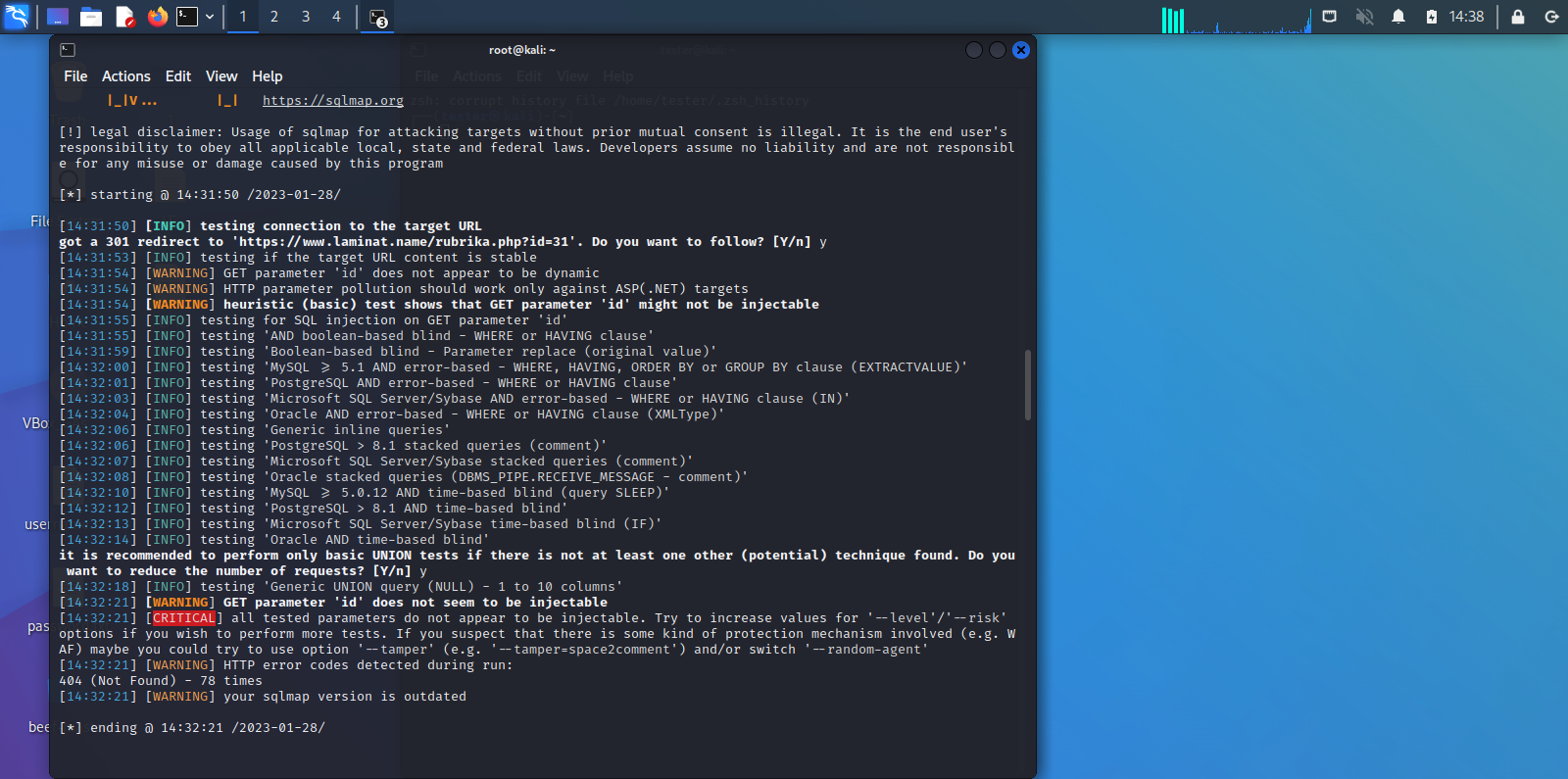
* + **--random-agent,**
  + **--randomize,**
  + **--hpp,**
  + **--risk (от 1 до 3, попробовать все, посмотреть разницу),**
  + **--os-pwn.**

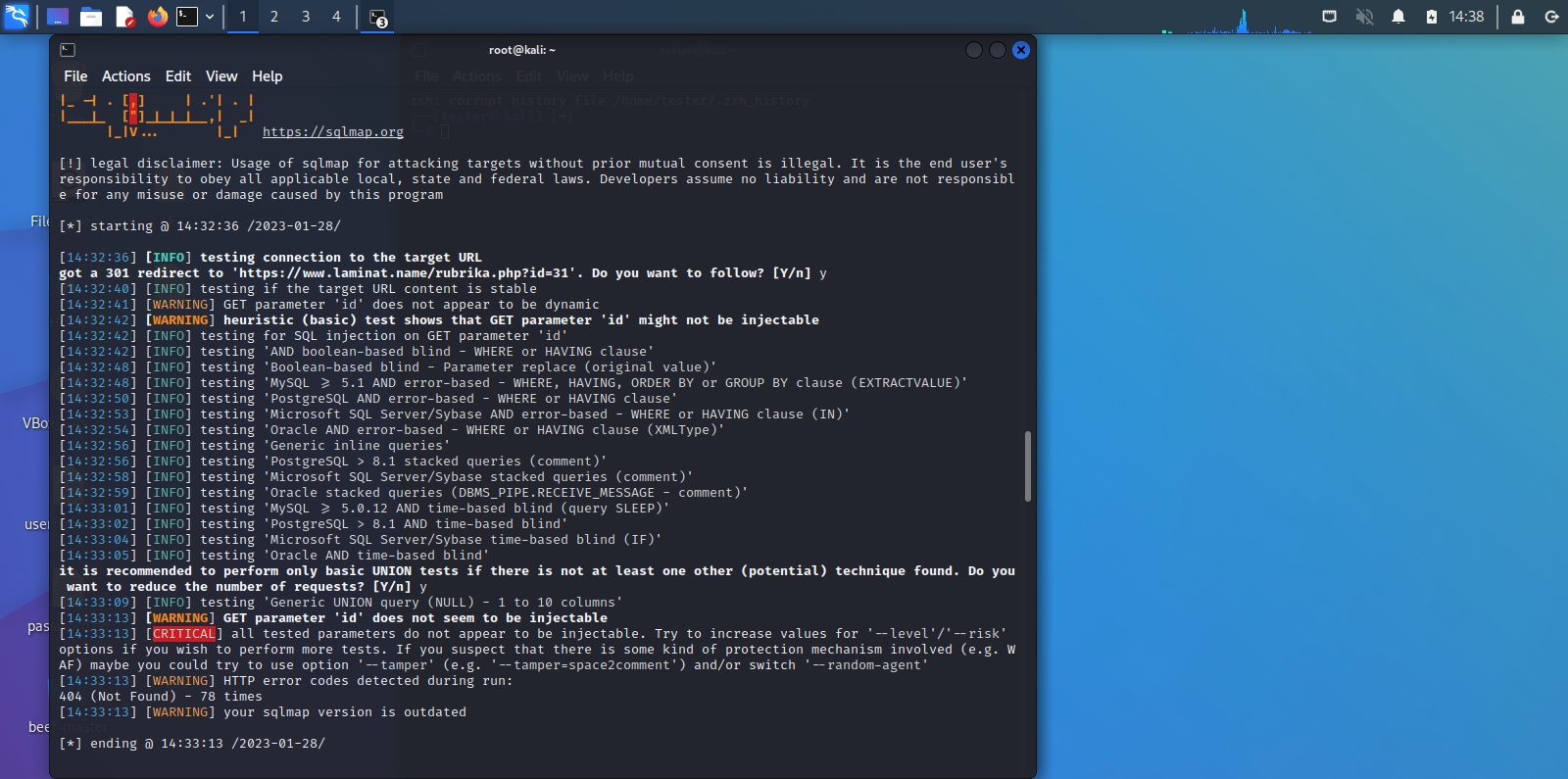
****

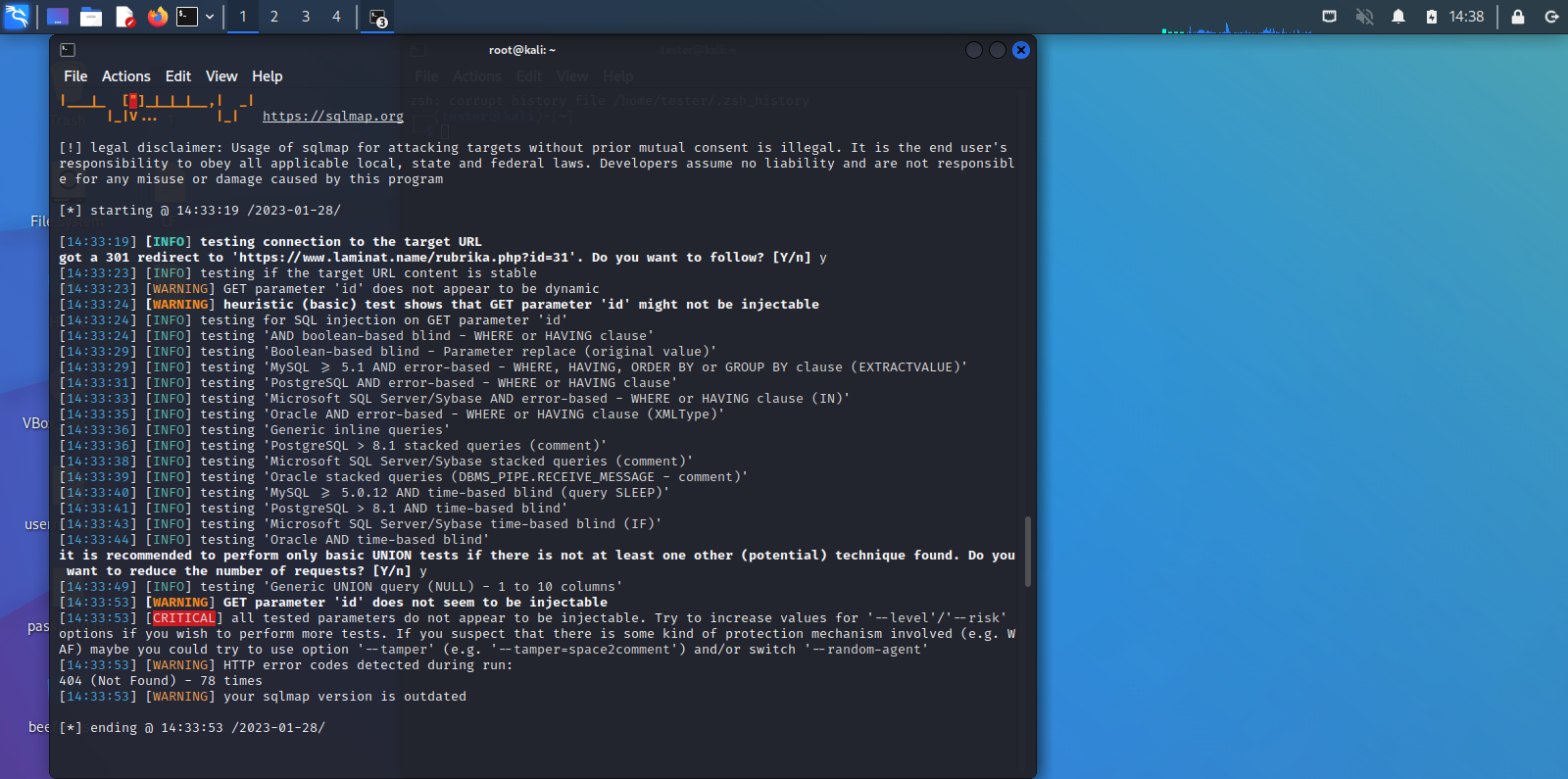
****

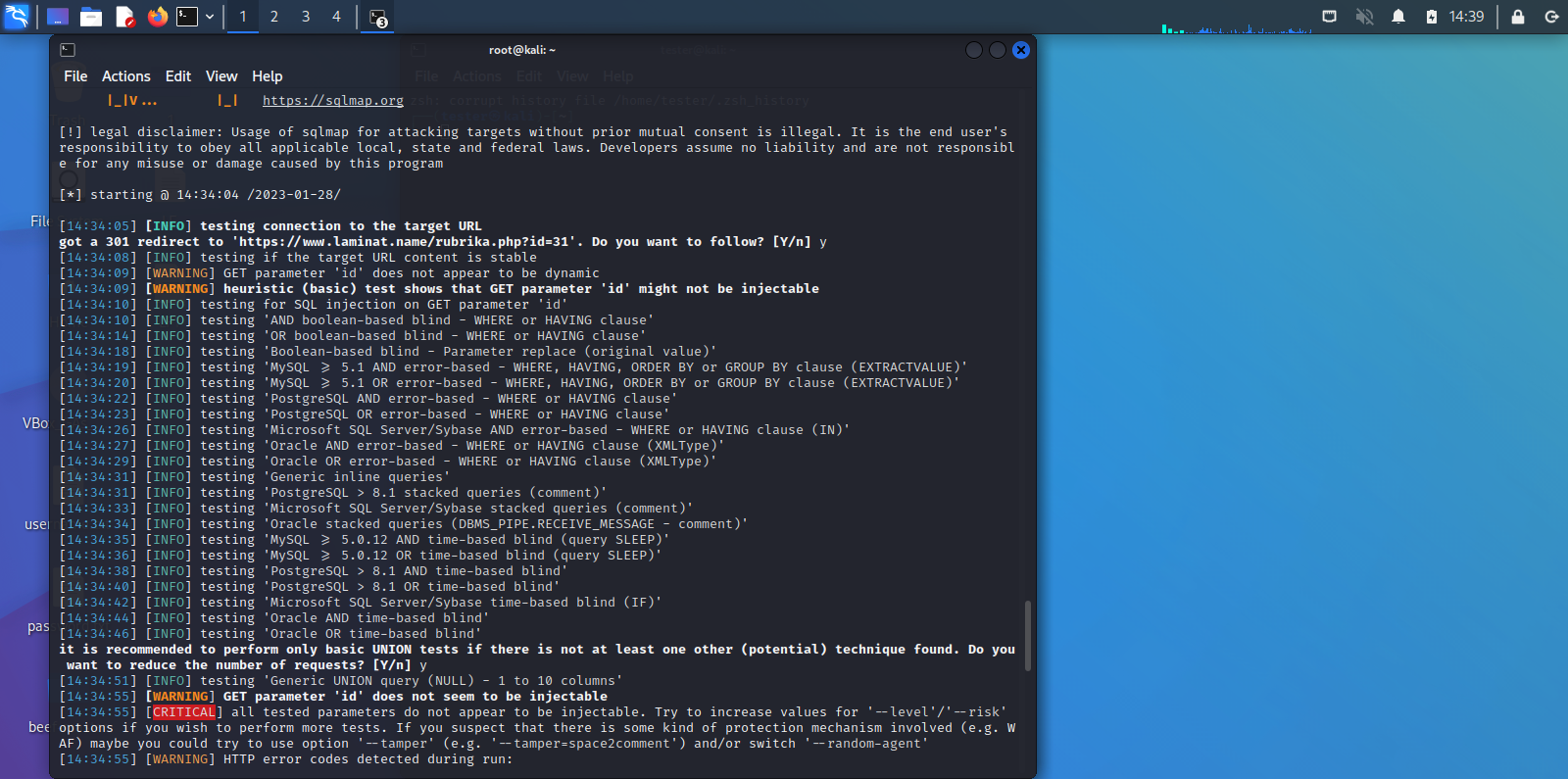
****

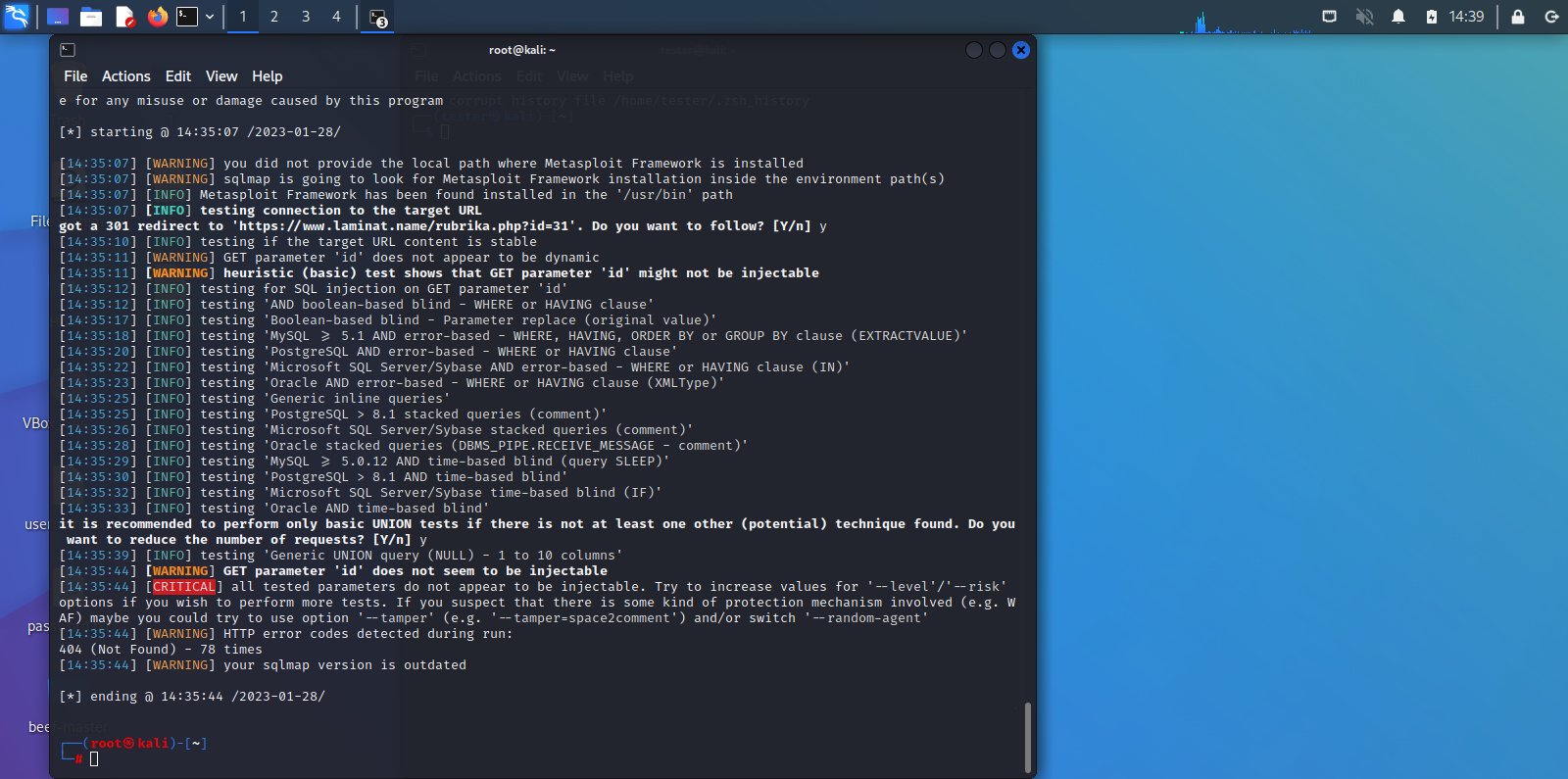
****

****

****

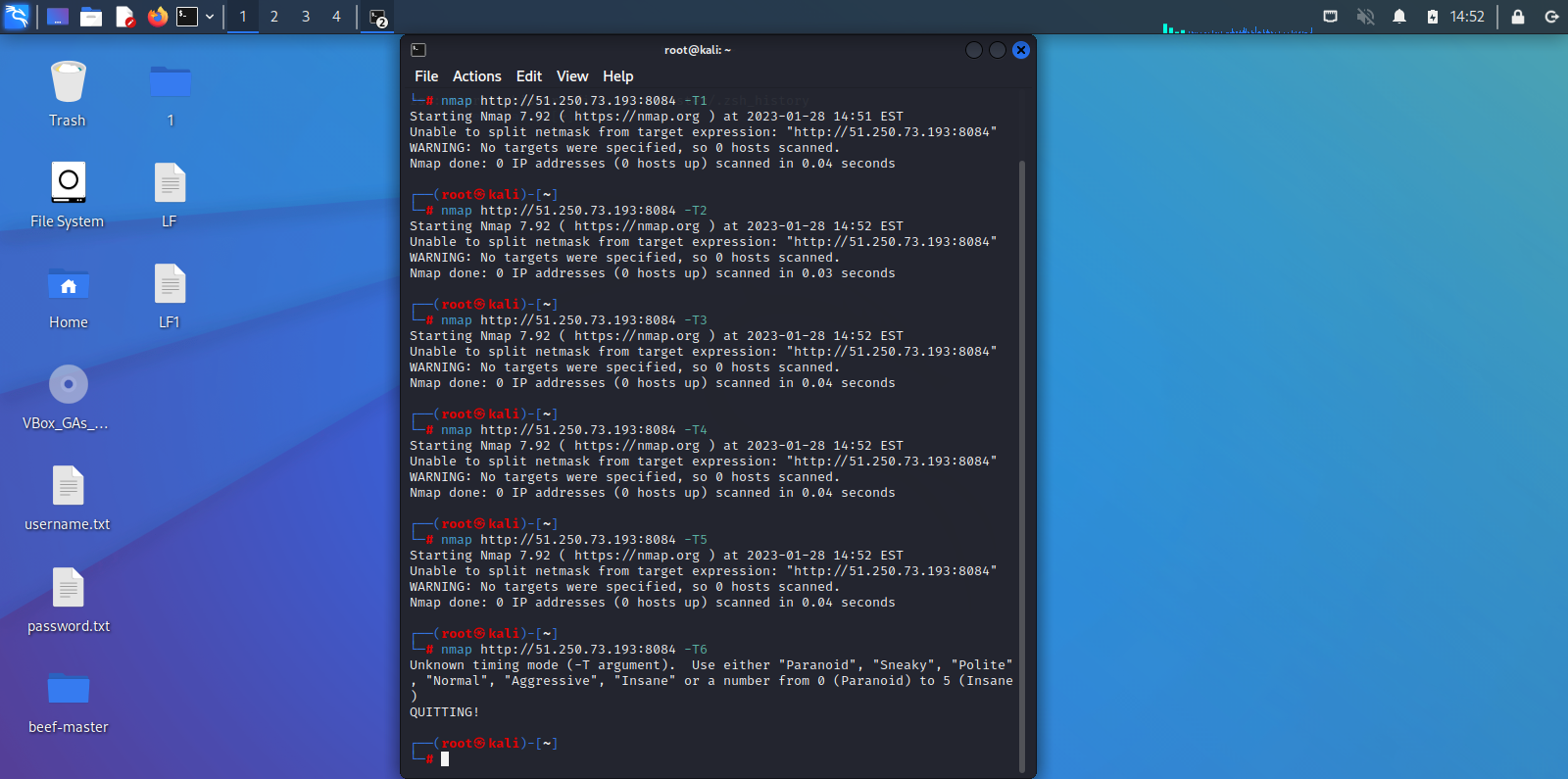
****

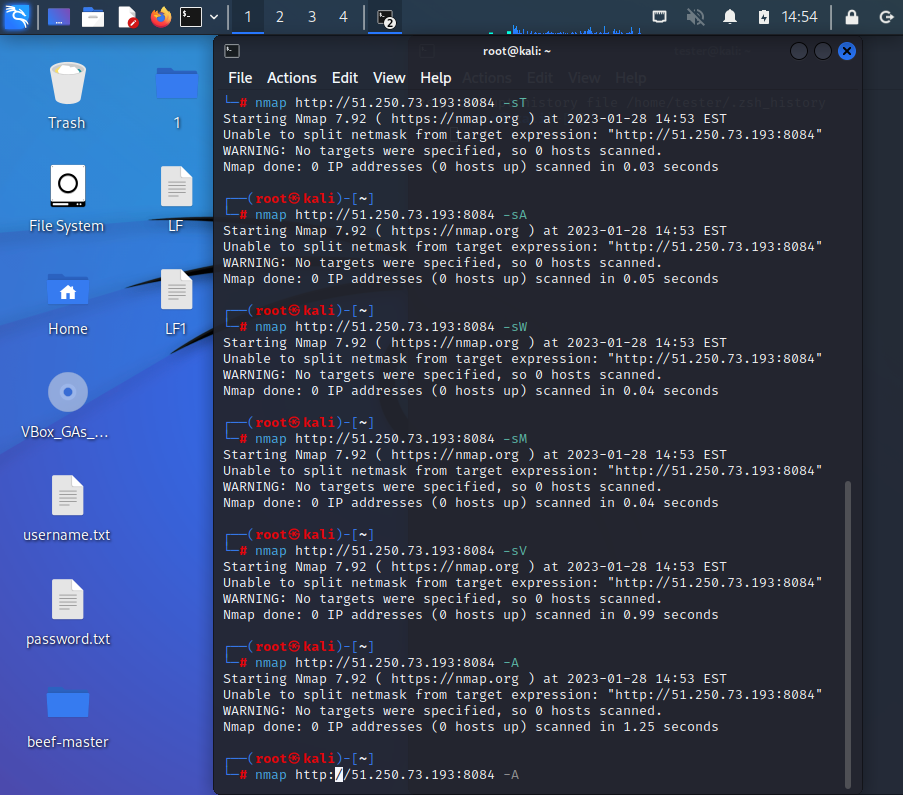
****

****

**NMAP**

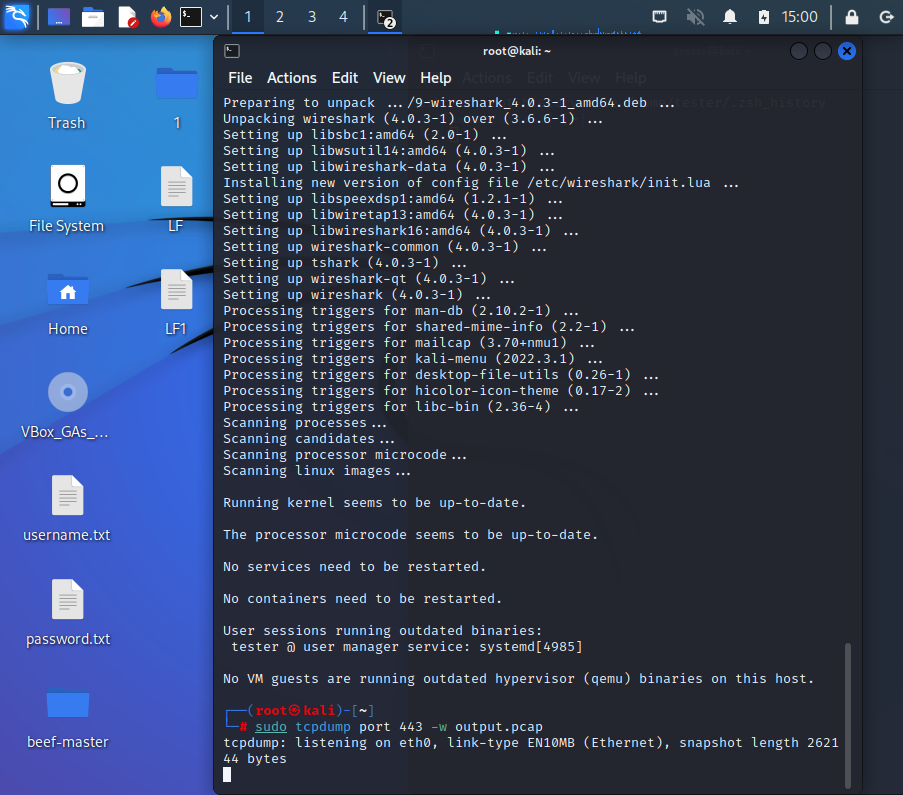
* **-T (от T1 до T6),**
* **-sS, -sT, -sA, -sW, -sM — применять разные типы сканирования, смотреть на их отличия в трафике,**
* **-sV — посмотреть, как nmap будет определять версии,**
* **-A.**

****

****

**Сделаю захват пакетов**

**sudo tcpdump port 443 -w output.pcap**

****

Процесс завис.

В результате, удалось поисследовать трафик с помощью утилит SQLMAP, NMAP, Wireshark.

Наиболее понятным инструментом для меня стал Wireshark, тк интуитивно понятный интерфейс, много полезных опций по фильтрации трафика. Можно легко проанализировать перегруженный трафик и проанализировать причину. Очень удобный режим просмотра пакетов — можно видеть необработанные данные пакета в виде последовательности байтов, и при наведении курсора мыши можно увидеть к какому полю оно относится.