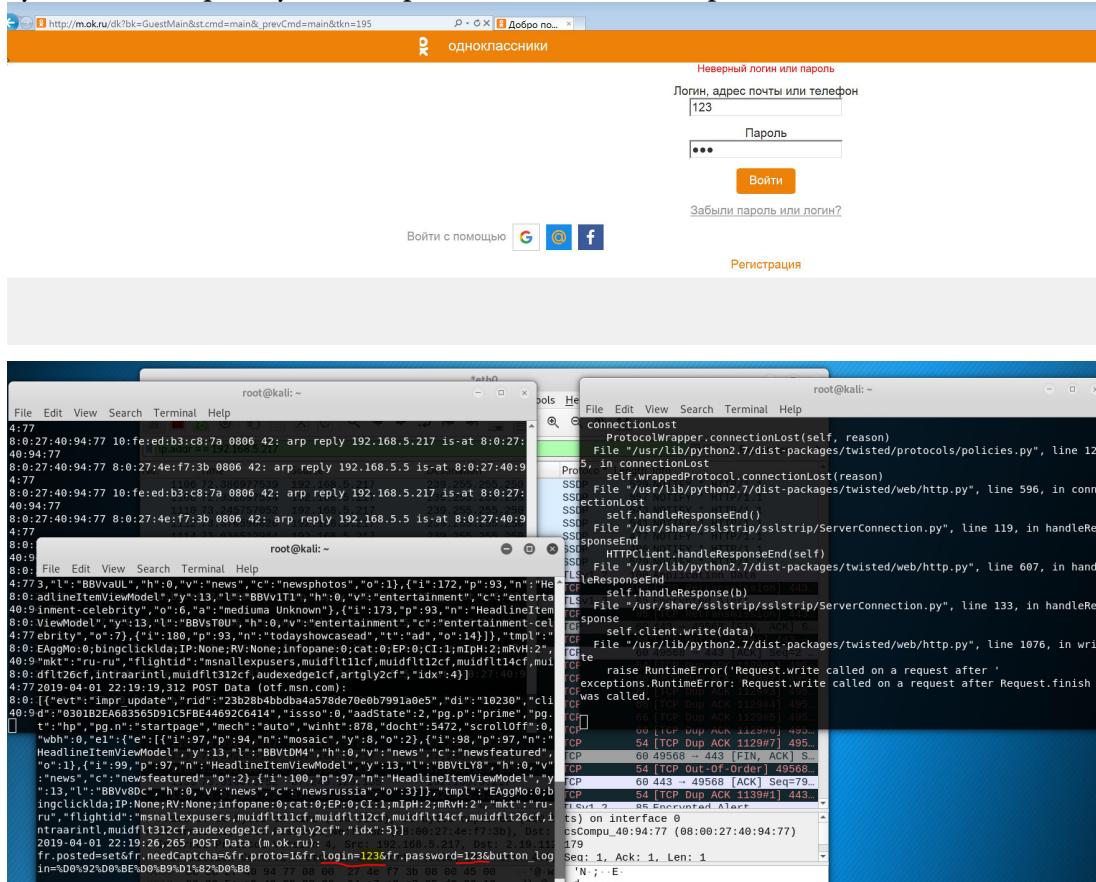


Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

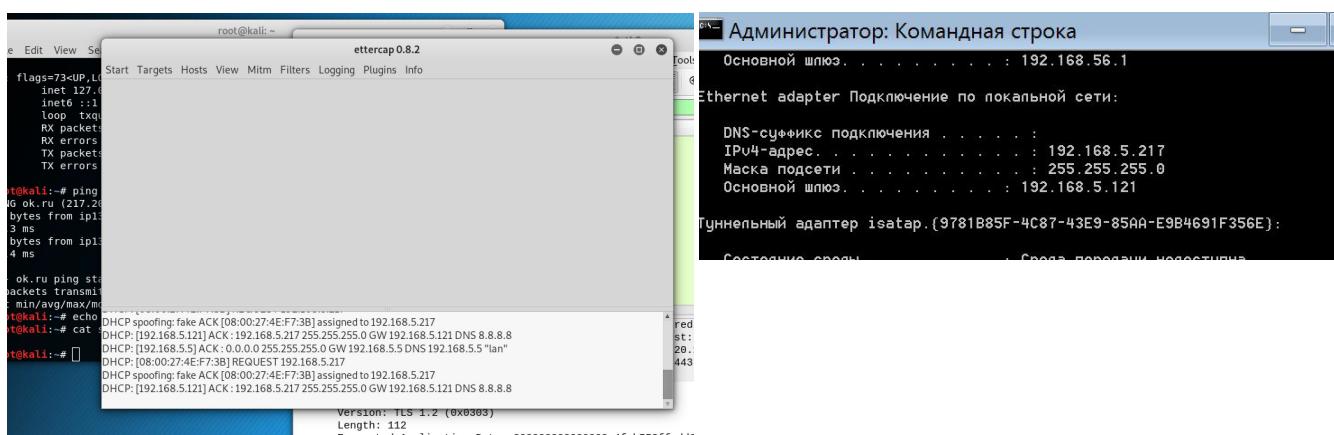
Задание 1: Выбрать сайт https и с помощью arpspoof перехватить данные, используя sslstrip. Сайт открыть в браузере жертвы.

Современные браузеры запоминают тег HSTS в ответе сервера, а так же некоторые браузеры имеют список предварительной загрузки, и из-за этого браузер никогда не перейдет на http. В результате sslstrip получается организовать только через IE11.



Задание 2*: Выполнить задание 1, используя dhcp spoof или yersinia. Разобраться, как работает dhcp spoofing, применяя Ettercap. С помощью ettercap -G запустить dhcp spoof, направив трафик жертвы на Kali linux. В Wireshark перехватить пароль на сайт https, который пытается посетить жертва.

Dhcp spoof провел через Ettercap. Ettercap перехватывая dhcp запросы, отвечает клиенту, что он есть dhcp сервер. И выдает ему из заранее заданного пула ip и является шлюзом для устройства. Получилось завернуть трафик на KaliLinux.



Каким образом осуществить перехват пароля по https не имея ключей и расшифровать его - идея не возникла. Единственное решение - записать лог sslkey и передать его в wireshark, данным способом получается, что необходим доступ к машине жертвы, для возможности создания переменной окружения, записи лога и перенаправления его на машину с KaliLinux.

The image shows the OK.RU login page. A woman with long brown hair, wearing an orange t-shirt with the word 'КОЭЭШБЭК' and a blue skirt, is laughing and playing a small guitar. The background is green. To her left is the OK.RU logo. To her right, there's text in Russian: 'На тарифе "Включайся! Выбирай"', a purple 'Подключить' button, and three circles (purple, purple, white) with a red '20%' overlay. Below the woman is the word 'МЕГАФОН'. On the right side, there's a login form with fields for 'Логин, адрес почты или телефон' (Login, email address or phone number) containing '123', 'Пароль' (Password) with an empty field, and an error message 'Неправильно указан логин и/или пароль' (Login and/or password entered incorrectly). Below the form are buttons for 'Вход' (Log in), 'Забыли пароль?' (Forgot password?), 'Регистрация' (Registration), and social media links for Google+, Email, and Facebook. At the bottom right, there's a small note about the 'OK.RU' logo and its history.