Взлом «админки» роутера

- Информационная безопасность

Здесь могло быть предупреждение о том, что не нужно пользоваться данной программой в преступных целях, но hydra это пишет перед каждым сеансом взлома

В общем, решил я по своим нуждам покопаться в настройках роутера, вбиваю я всем знакомый адрес, а тут пароль спрашивают. Как быть? Ну, начал я перебирать пароли, а их количество слишком большое, что бы перебирать все и слишком маленькое, чтобы делать reset.

И я открыл google. После пары запросов я узнал о такой вещи как hydra. И тут началось: жажда открытий, поиски неизведанного и так далее.

Приступим

Первым делом мной был составлен словарь паролей, ни много, ни мало, аж на 25 комбинаций. Далее качаем либо Kali linux, либо саму Гидру (если ~~вы пингвин~~ у вас линукс). Теперь у нас два варианта (ну как два, я нашел информацию по двум вариантам).

Либо у вас вот такое диалоговое окно:

Либо логин и пароль запрашивает форма на сайте. Мой вариант первый, поэтому начнем с него. На нашем пути к «админке» стоит страж в виде диалогового окна. Это вид авторизации **http-get.**

Открываем терминал. Вводим:

```
hydra -l admin -P myPass.txt -s 80 192.168.1.1 http-get /
```

Где после «-l» идет логин, после «-P» словарь, после «-s» порт. Также в нашем распоряжении есть другие флаги:

-R восстановить предыдущую прерванную/оборванную сессию

-S выполнить SSL соединение

-s ПОРТ если служба не на порту по умолчанию, то можно задать порт здесь

-l ЛОГИН или -L ФАЙЛ с ЛОГИНАМИ (именами), или загрузить несколько логинов из ФАЙЛА

-p ПАРОЛЬ или -P ФАЙЛ с паролями для перебора, или загрузить несколько паролей из ФАЙЛА

-x МИНИМУМ: МАКСИМУМ: НАБОР_СИМВОЛОВ генерация паролей для брутфорса, наберите "-x -h" для помощи

-e nsr «n» — пробовать с пустым паролем, «s» — логин в качестве пароля и/или «r» — реверс учётных данных

-u зацикливаться на пользователя, а не на парлях (эффективно! подразумевается с использованием опции -x)

-C ФАЙЛ формат где «логин: пароль» разделены двоеточиями, вместо опции -L/-P

-M ФАЙЛ список серверов для атак, одна запись на строку, после двоеточия ':' можно задать порт

-o ФАЙЛ записывать найденные пары логин/пароль в ФАЙЛ вместо стандартного вывода

-f / -F выйти, когда пара логин/пароль подобрана (-M: -f для хоста, -F глобально)

-t ЗАДАЧИ количество запущенных параллельно ЗАДАЧ (на хост, по умолчанию: 16)

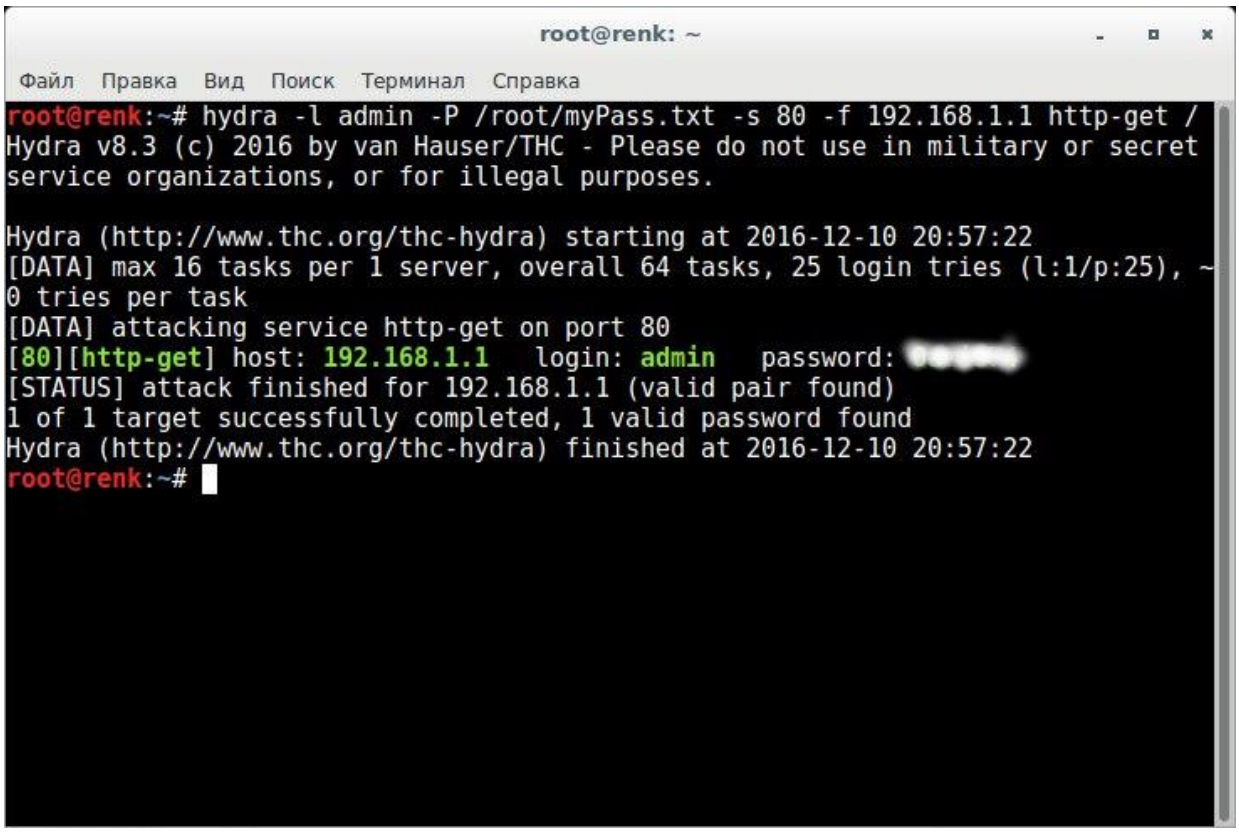
-w / -W ВРЕМЯ время ожидания ответов (32 секунды) / между соединениями на поток
-4 / -6 предпочитать IPv4 (по умолчанию) или IPv6 адреса

-v / -V / -d вербальный режим / показывать логин+пароль для каждой попытки / режим отладки

-q не печатать сообщения об ошибках соединения

-U подробные сведения об использовании модуля
server цель: DNS, IP или 192.168.0.0/24 (эта ИЛИ опция -M)
service служба для взлома (смотрите список поддерживаемых протоколов)
OPT некоторые модули служб поддерживают дополнительный ввод (-U для справки по модулю)

Ну вот так как-то:



Второй вариант:

Не мой, честно взят с Античата, с исправлением грамматических ошибок автора (Обилие знаков пунктуации я оставил). Интересно это можно считать переводом?

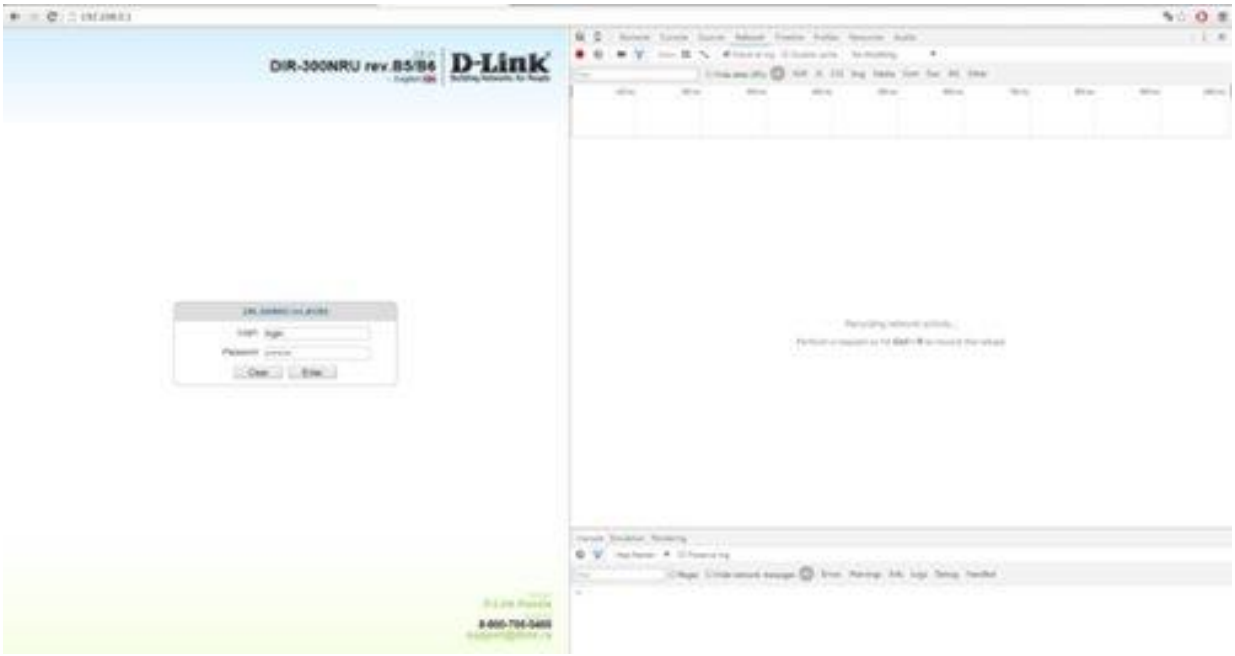
Нас встречает форма на сайте:

Такой метод авторизации — **http-post-form**, и тут нужно немного повозится, так как нам нужно понять, как браузер отправляет роутеру данные.

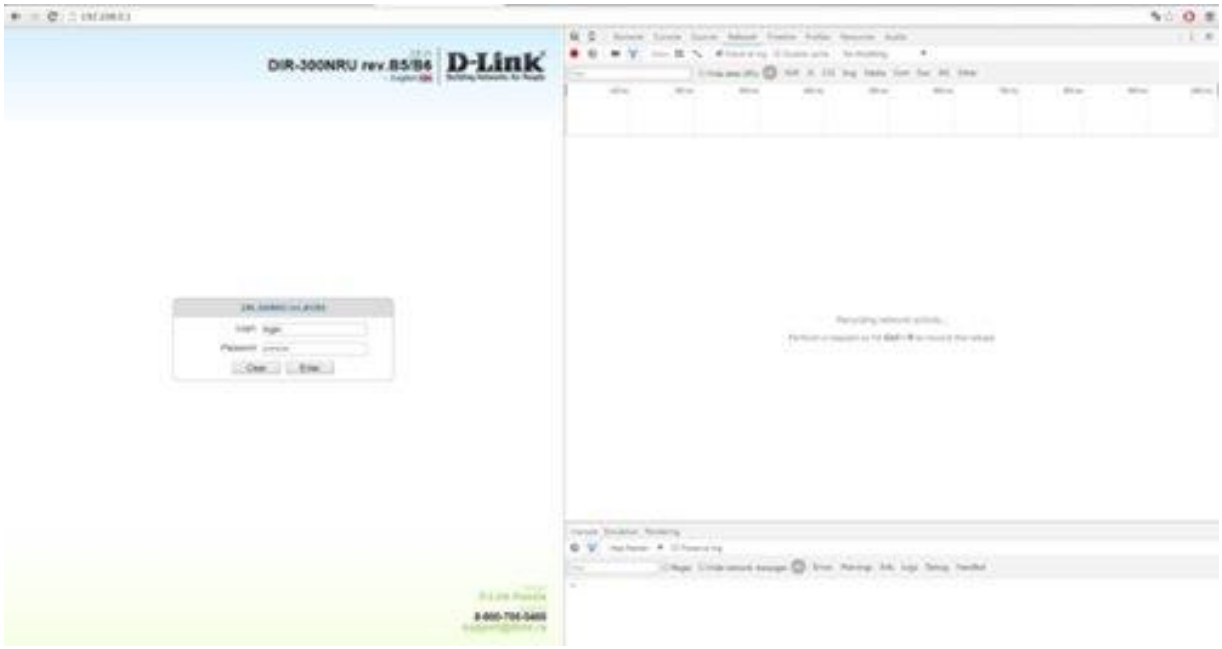
В данном случае и использовал браузер Chrome (его аналог Chromium в Kali Linux, ставится через apt-get install chromium).

Сейчас нужно сделать одну очень глупую вещь… указать неверный логин и пасс…
для чего увидим позже…

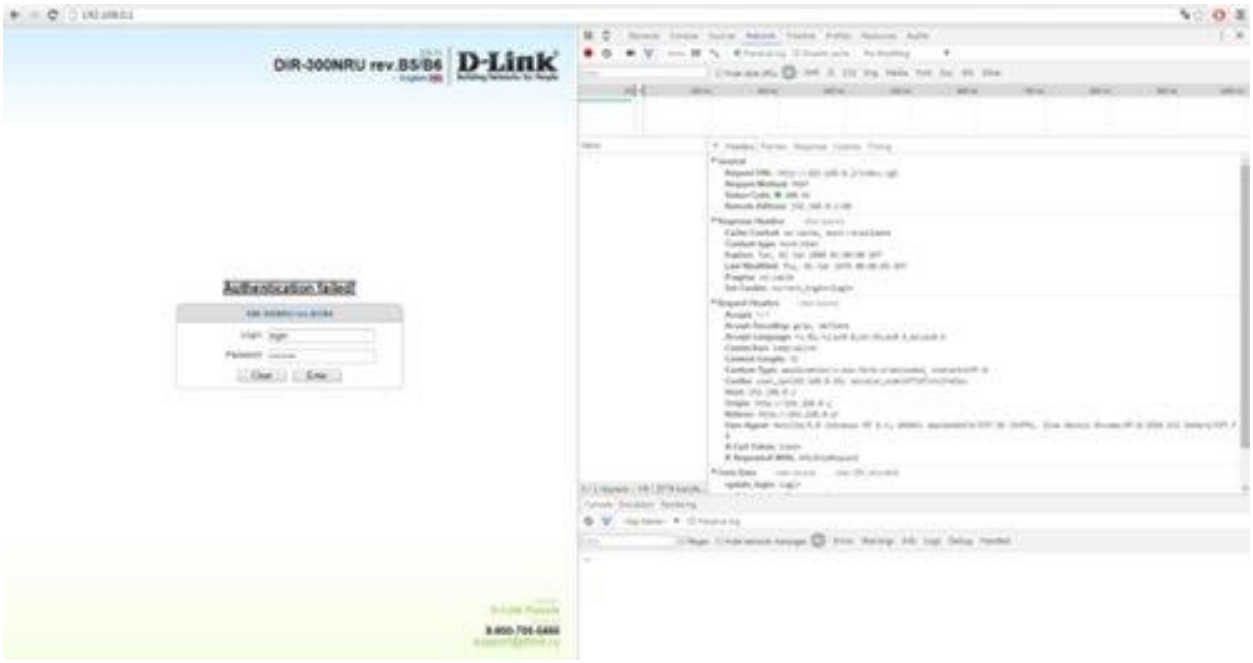
Нажимаем F12 что бы перейти в режим редактирования веб-страницы.



Переходим в Network → Включаем галочку **Preserv log**.



Вводим ложные логин и пароль…

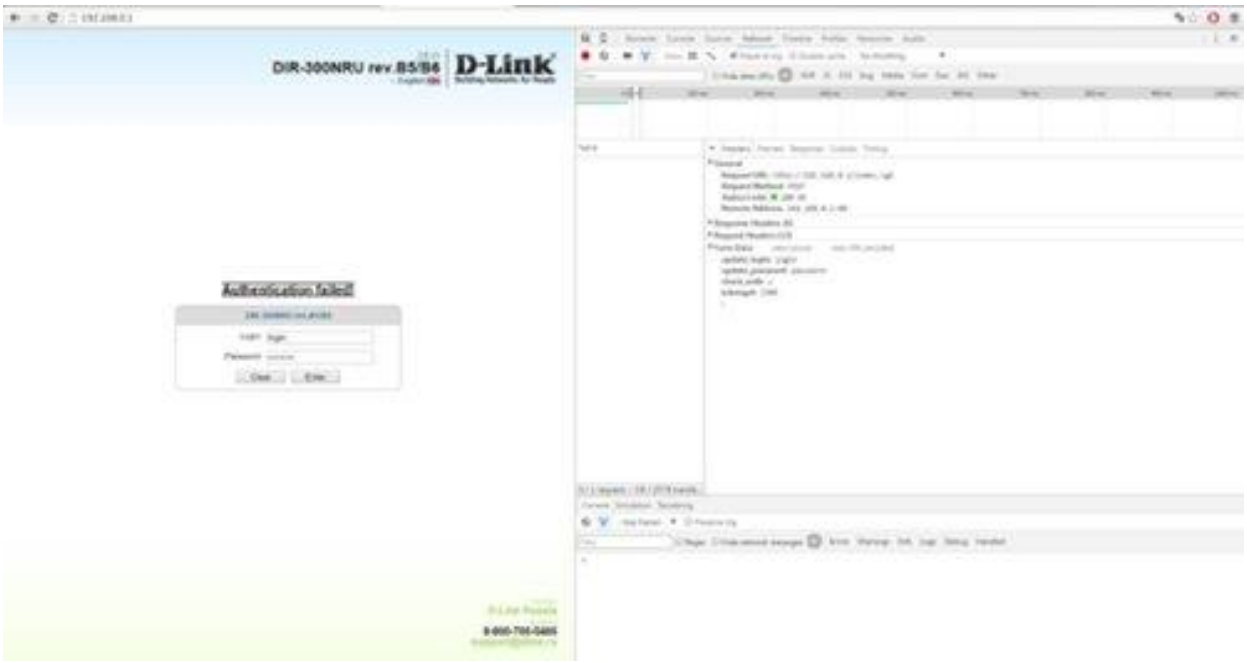


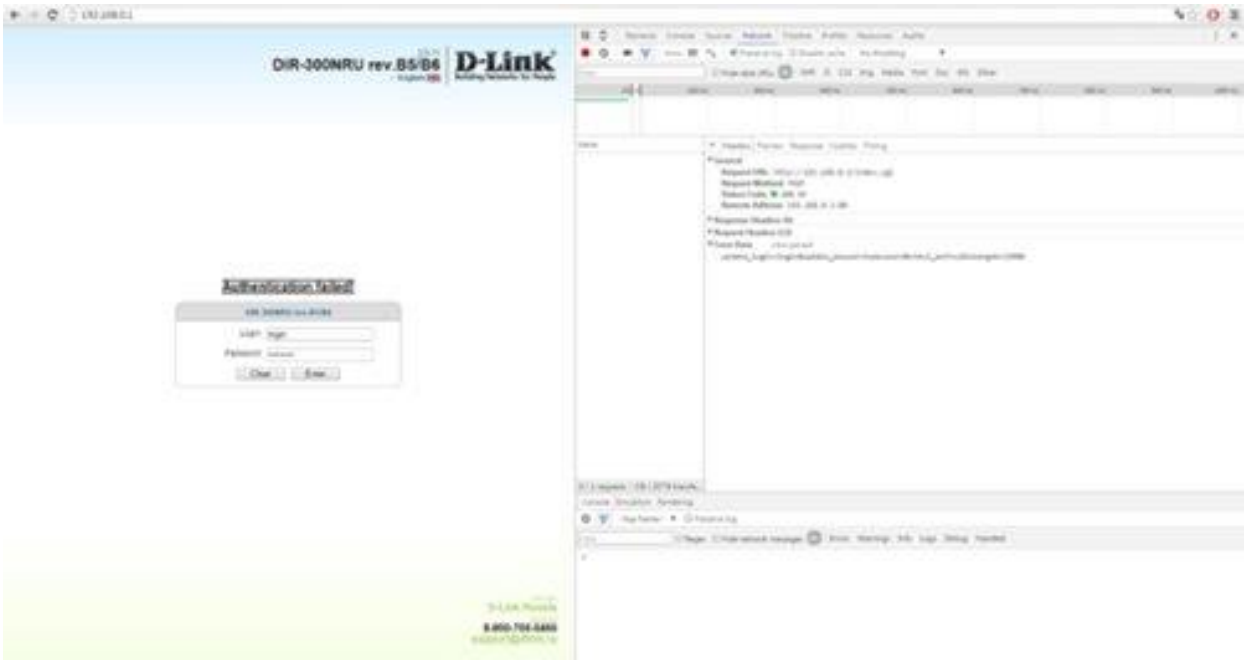
Ну что за дела? Так не пойдет! Более того, после нескольких неудачных попыток входа, форма блокируется на 180 секунд.

Переходим во вкладочку **HEADERS** ищем строку:

```
Request URL:http://192.168.0.1/index.cgi
```

Отрезаем все до ip-адреса — /index.cgi… Поздравляю мы нашли первую часть скрипта авторизации… Идем дальше… Переходим к вкладке **FORM DATA** и изменяем режим отображения на **VIEV SOURCE**.

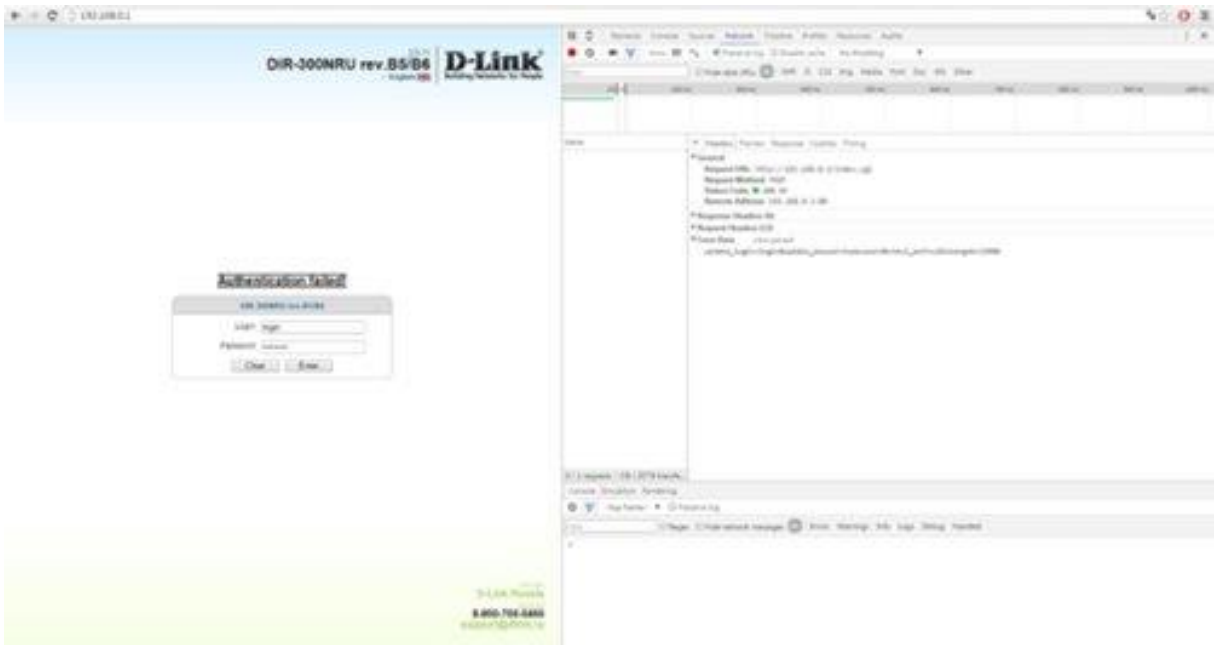





```
update_login=login&update_password=password&check_auth=y&tokenget=1300&
```

```
update_login=login&update_password=password
```

Бинго! Мы нашли вторую часть скрипта авторизации! Еще чуть-чуть! теперь нужно найти страницу с сообщением об ошибке... Нужно нажать на вкладку ELEMENTS.



И выбрать элемент HTML кода (CTRL+SHIFT+C) и выбрать окно с сообщением об ошибки... в данном случае — Authentication failed!


```
<span langkey="bad_auth" style="display: inline;">Authentication failed!
</span>
```

Выбираем:

```
span langkey="bad_auth"
```

и немножко правим… bad_auth — все! Ключ практически у нас в кармане… Теперь мы можем полностью написать строку авторизации:

```
index.cgi:update_login=login&update_password=password:bad_auth
```

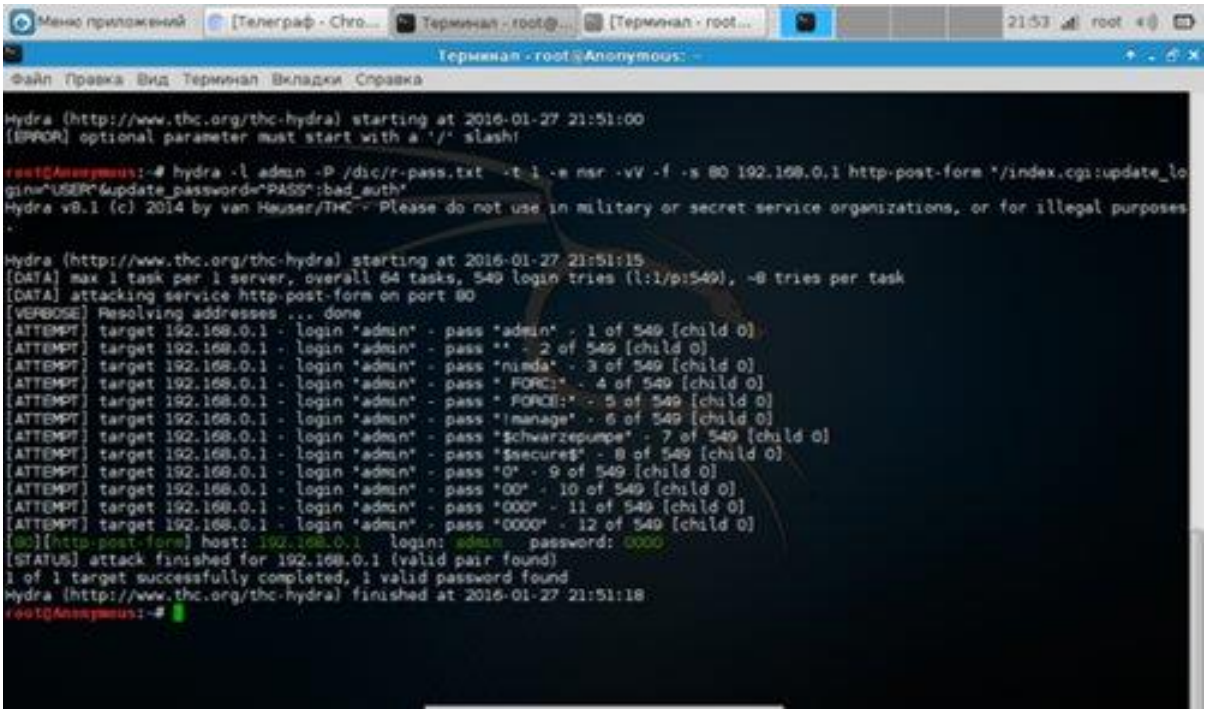
Теперь нужно подставить вместо «login» — ^USER^ и вместо «password» ^PASS^ и тогда строка будет иметь вид:

```
index.cgi:update_login=^USER^&update_password=^PASS^:bad_auth
```

Вводим команду:

```
hydra -l admin -P router-pass.dic -t 1 -e nsr -vV -f -s 80 192.168.0.1 h
ttp-post-form "/index.cgi:update_login=^USER^&update_password=^PASS^:bad
_auth"
```

Обратите внимание что между частями скрипта двоеточие! это обязательно! Кстати, блокировки формы через гидру не происходило… Это очень радует.



В работоспособности второго метода мне убедиться не светит, так как я не обладатель подходящей модели роутера. Придется довериться экспрессивному человеку с Античата.

Если кому интересно, будьте добры, проверьте и отпишитесь в комментариях. Я работал с роутером TL-WR1043N/TL-WR1043ND. Роутер с Античата — D-link300NRU.