

## Задание выполнил студент группы 2345 Романенко К.Д.

1. Ознакомиться с кодировкой base64.

С помощью Base64 можно взять любую форму данных и преобразовать её в строку обычного текста для отправки через интернет или любой другой носитель без повреждения данных.

2. Провести аудит сетевого трафика. Скачать дамп .pcap, приложенный к уроку. Проанализировать трафик, найти секретное послание. Отчет приложить к домашнему заданию.

1. Перешёл в папку со скачанным дампом

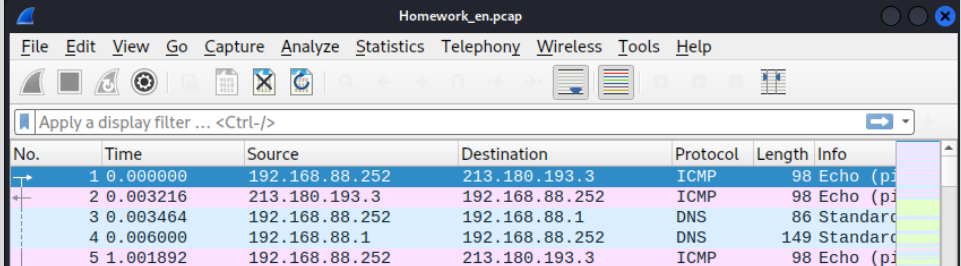
```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
# cd /home/kali/Downloads/

(root㉿kali)-[/home/kali/Downloads]
# ls
Homework_en.pcap

(root㉿kali)-[/home/kali/Downloads]
#
```

2. Отправил дамп в Wireshark с -r

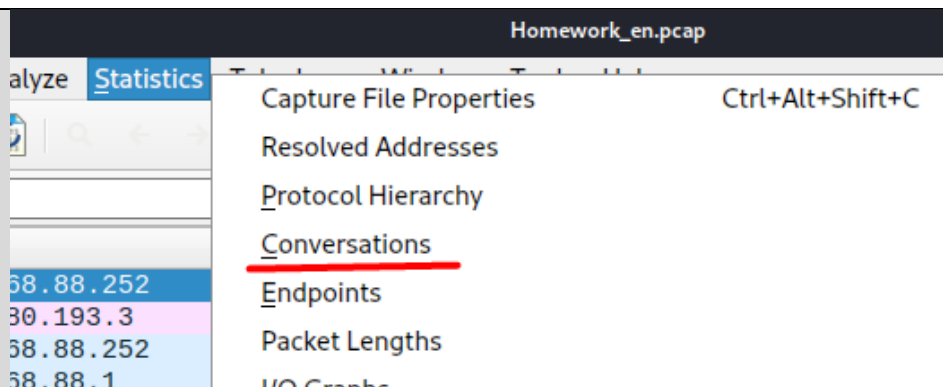
```
(root㉿kali)-[/home/kali/Downloads]
# wireshark -r Homework_en.pcap
** (wireshark:5402) 11:19:12.229498 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting
```



The screenshot shows the Wireshark interface with the file 'Homework\_en.pcap' loaded. The packet list pane displays five packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.88.252	213.180.193.3	ICMP	98	Echo (ping) request
2	0.003216	213.180.193.3	192.168.88.252	ICMP	98	Echo (ping) reply
3	0.003464	192.168.88.252	192.168.88.1	DNS	86	Standard query type
4	0.006000	192.168.88.1	192.168.88.252	DNS	149	Standard query response
5	1.001892	192.168.88.252	213.180.193.3	ICMP	98	Echo (ping) request

3. Перешёл к Статистике диалогов (Statistics – Conversations), чтобы изучить незашифрованную информацию



И фильтрую по порту В (порт назначения)

Ethernet · 6	IPv4 · 61	IPv6 · 3	<u>TCP · 142</u>	UDP · 475
Address A	Port A	Address B	Port B ▾	Packets
192.168.88.252	47106	192.168.88.1	21	55
192.168.88.252	47845	132.247.30.101	25	35
192.168.88.252	44482	5.9.242.204	80	15
192.168.88.252	52692	62.115.255.198	80	7
192.168.88.252	52713	62.115.255.198	80	6
192.168.88.252	39847	62.161.94.220	80	10
192.168.88.252	39848	62.161.94.220	80	10

Используемые порты: 21, 25, 80 и 443. Особый интерес представляет 25, т.к. это SMTP. Там может быть флаг.

#### 4. С помощью display filter ищу SMTP

No.	smtp	Source	Destination	Protocol
2156	44.887373	132.247.30.101	192.168.88.252	SMTP
2326	64.404295	192.168.88.252	132.247.30.101	SMTP
2328	64.672058	132.247.30.101	192.168.88.252	SMTP
2423	76.584130	192.168.88.252	132.247.30.101	SMTP
2425	76.804173	132.247.30.101	192.168.88.252	SMTP

При анализе вижу, что from Alice to Bob пришло письмо

SMTP	72 S: 2500
TCP	66 47845 → 25 [ACK] Seq=22 Ack=29 Win=29312 Len=0 TSval=5049781 ...
SMTP	92 C: MAIL FROM: <u>alice@mail.ru</u>
TCP	66 25 → 47845 [ACK] Seq=29 Ack=48 Win=14480 Len=0 TSval=37527897...
SMTP	74 S: 250 OK
TCP	66 47845 → 25 [ACK] Seq=48 Ack=37 Win=29312 Len=0 TSval=5052814 ...
SMTP	92 C: RCPT TO: <u>bob@gov.mail.ru</u>
SMTP	74 S: 250 OK

и его текст

2914	164.017540	192.168.88.252	132.247.30.101	SMTP/IMF	69 Hello,Bob! I put this file to our file share
2924	165.875850	192.168.88.252	132.247.30.101	SMTP	68 C: DATA fragment, 2 bytes
2925	166.094808	132.247.30.101	192.168.88.252	SMTP	104 S: 250 OK: Queued message as 642384918c
2931	166.372489	192.168.88.252	132.247.30.101	SMTP	69 C: DATA fragment, 3 bytes
2932	166.593167	132.247.30.101	192.168.88.252	SMTP	101 S: 502 Error: command not recognized
2946	169.338913	192.168.88.252	132.247.30.101	SMTP	72 C: QUIT
2947	169.559400	132.247.30.101	192.168.88.252	SMTP	75 S: 221 Bye

Frame 2914: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)	0000	4c 5e 0c c3 dd 8b 8
Ethernet II, Src: VMware_67:2f:26 (00:0c:29:67:2f:26), Dst: Routerbo_c3:dd:8b (4c:5e:0c:c3:dd:8b)	0010	00 37 70 21 40 00 4
Internet Protocol Version 4, Src: 192.168.88.252, Dst: 132.247.30.101	0020	1e 65 ba e5 00 19 2
Transmission Control Protocol, Src Port: 47845, Dst Port: 25, Seq: 203, Ack: 78, Len: 3	0030	00 e5 bd 2a 00 00 0
Simple Mail Transfer Protocol	0040	f5 17 2e 0d 0a
Internet Message Format		
Message Text		
Hello,Bob! I put this file to our file share, as always. That file, you know... Please, dow		

Чтобы убедиться, что адресат и получатель определил верно:  
ЛКМ на строку с письмом -> ПКМ -> Follow -> TCP Stream

```

220 SMTP Corp Server
EHLO 132.247.30.101
250
MAIL FROM: alice@mail.ru
250 OK
RCPT TO: bob@gov.mail.ru
250 OK
DATA
354 Enter message, end with "."
Hello,Bob! I put this file to our file share, as always. That file, you know... Please,
download it and take a look. Bye!
.
250 OK: Queued message as 642384918c
.
502 Error: command not recognized
QUIT
221 Bye

```

В диалоге речь идёт о шаре. Ищу дальше.

## 5. Протокол ftp

Внёс новый фильтр. Сразу нашёл данные УЗ admin

No.	Time	Source	Destination	Protocol	Length Info
3136	188.642245	192.168.88.1	192.168.88.252	FTP	113 Response: 220 MikroTik FTP server (MikroTik 6.27) ready
3152	192.039316	192.168.88.252	192.168.88.1	FTP	78 Request: USER admin
3154	192.040202	192.168.88.1	192.168.88.252	FTP	99 Response: 331 Password required for admin
3186	199.152596	192.168.88.252	192.168.88.1	FTP	81 Request: PASS pa\$w0rd
3188	199.180723	192.168.88.1	192.168.88.252	FTP	92 Response: 230 User admin logged in
3190	199.189112	192.168.88.252	192.168.88.1	FTP	72 Request: SYST
3192	199.189673	192.168.88.1	192.168.88.252	FTP	90 Response: 215 UNIX MikroTik 6.27
3210	203.062930	192.168.88.252	192.168.88.1	FTP	95 Request: PORT 192,168,88,252,209,126
3211	203.063098	192.168.88.1	192.168.88.252	FTP	95 Response: 200 PORT command successful
3213	203.063271	192.168.88.252	192.168.88.1	FTP	72 Request: LIST
3217	203.064888	192.168.88.1	192.168.88.252	FTP	95 Response: 150 Opening data connection
3225	203.068903	192.168.88.1	192.168.88.252	FTP	89 Response: 226 Transfer complete
3282	215.374446	192.168.88.252	192.168.88.1	FTP	77 Request: QUIT

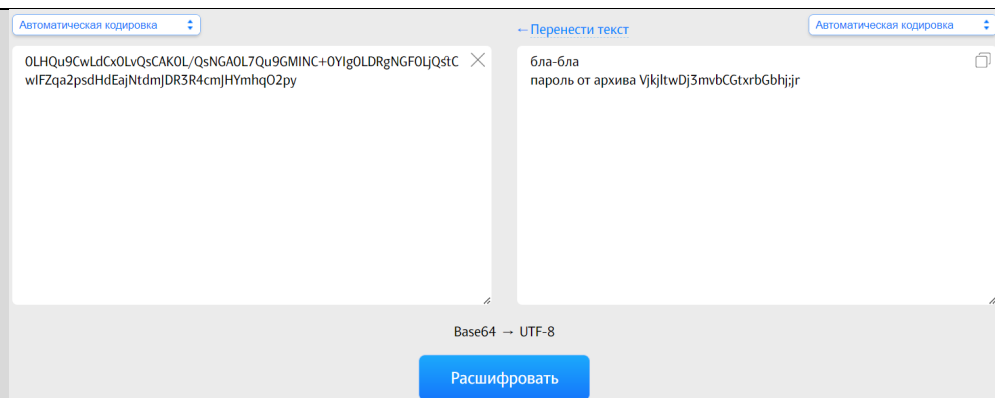
## 6. Но разговор шёл о файле и шаре. Ищу дальше. FTP-DATA

No.	Time	Source	Destination	Protocol	Length Info
3218	203.067481	192.168.88.1	192.168.88.252	FTP-DATA	121 FTP Data: 55 bytes (PORT) (LIST)
3220	203.068103	192.168.88.1	192.168.88.252	FTP-DATA	226 FTP Data: 100 bytes (PORT) (LIST)
3341	222.621788	192.168.88.1	192.168.88.252	FTP-DATA	121 FTP Data: 55 bytes (PORT) (LIST)
3342	222.621799	192.168.88.1	192.168.88.252	FTP-DATA	226 FTP Data: 100 bytes (PORT) (LIST)
3394	232.283479	192.168.88.1	192.168.88.252	FTP-DATA	161 FTP Data: 95 bytes (PORT) (RETR urgent_file.txt)

Вижу файл urgent\_file.txt

ПКМ -> Follow -> TCP Stream

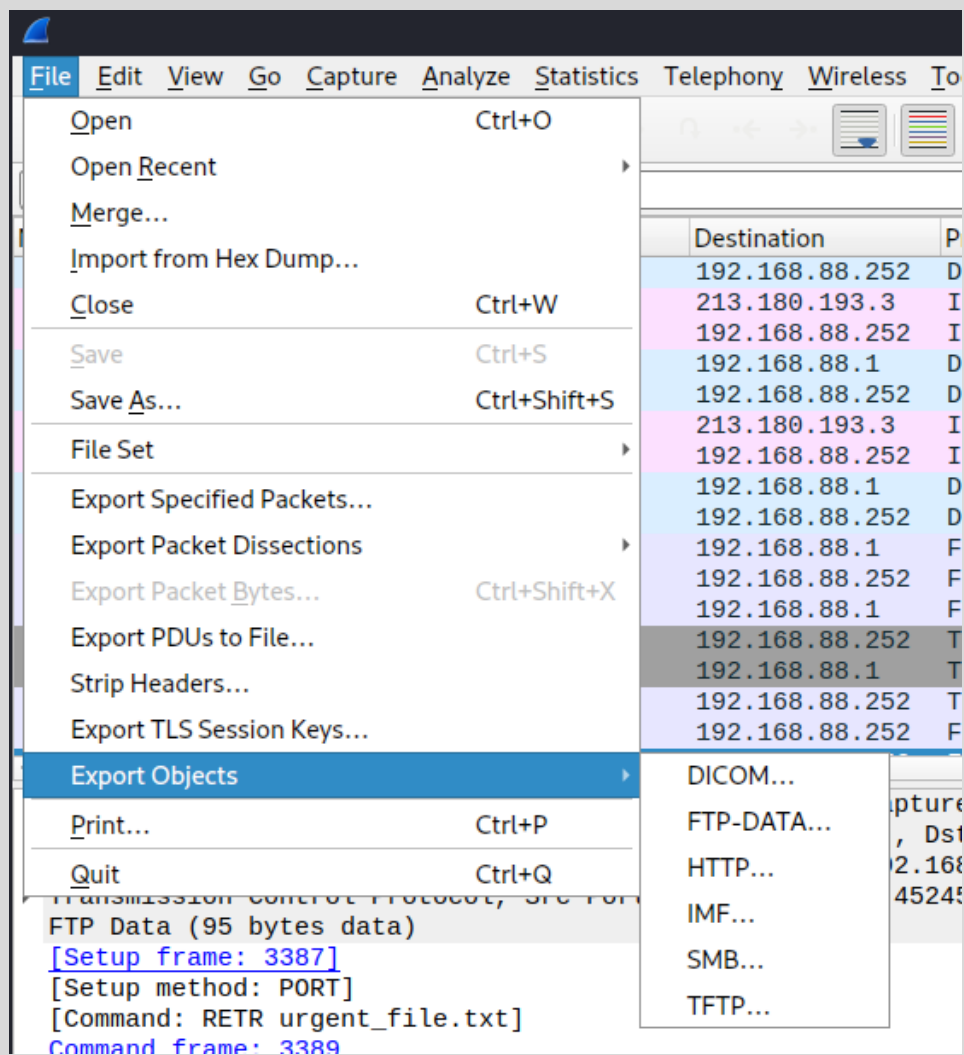




Пароль от архива: VjkjltwDj3mnbCGtxrbGbhj;jr

9. Раз есть пароль от архива и есть информация про файл на шаре, то ищу файл

Смотрю всё, что передавалось по HTTP



Раз это архив, значит файл. Нашёл интересную строку с информацией о загрузке файла

180	suggest.yandex.ru	text/javascript	375 bytes	suggest-ya.cgi?callback=jQuery183032242646179407564_
195	suggest.yandex.ru	text/javascript	375 bytes	suggest-ya.cgi?callback=jQuery183032242646179407564_
4147	www.filedropper.com	application/octet-stream	260 bytes	filedownload.php?id=loot
1484	www.rbc.ru	application/json	207 bytes	pollrpc
1640	suggest.yandex.ru	text/javascript	205 bytes	suggest-ya.cgi?callback=jQuery183044122853725054534_
1648	suggest.yandex.ru	text/javascript	205 bytes	suggest-ya.cgi?callback=jQuery183044122853725054534_

отфильтровал по filedropper

Packet	Hostname	Content Type	Size	Filename
3740	www.filedropper.com	application/x-shockwave-flash	23 kB	336x280hivelocity.swf
3628	www.filedropper.com	text/html	8,897 bytes	loot
3709	www.filedropper.com	image/png	3,874 bytes	securimage_show.php?sid=b672ce7be54c97bf7ec375b3c7c2
4147	www.filedropper.com	application/octet-stream	260 bytes	filedownload.php?id=loot
4140	www.filedropper.com	application/x-www-form-urlencoded	9 bytes	filedownload.php?id=loot

По 4140 что-то зашло, а по 4147 пришёл отчёт о выполнении

4139	260.621752	192.168.88.252	74.50.120.88	TCP	66 59943 → 80 [ACK] Seq=1 Ack=1 Win=29312
4140	260.622221	192.168.88.252	74.50.120.88	HTTP	761 POST /processing/filedownload.php?id=loot
4141	260.642400	74.50.120.88	192.168.88.252	TCP	74 80 → 59944 [SYN, ACK] Seq=0 Ack=1 Win=
4142	260.642460	192.168.88.252	74.50.120.88	TCP	66 59944 → 80 [ACK] Seq=1 Ack=1 Win=29312
4143	261.062545	192.168.88.252	74.50.120.88	TCP	761 [TCP Retransmission] 59943 → 80 [PSH, A
4144	261.097168	74.50.120.88	192.168.88.252	TCP	730 80 → 59943 [PSH, ACK] Seq=1 Ack=696 Win=
4145	261.097235	192.168.88.252	74.50.120.88	TCP	66 59943 → 80 [ACK] Seq=696 Ack=665 Win=36
4146	261.219299	74.50.120.88	192.168.88.252	TCP	78 [TCP Dup ACK 4144#1] 80 → 59943 [ACK] S
4147	261.270633	74.50.120.88	192.168.88.252	HTTP	71 HTTP/1.1 200 OK

Смотрю Follow -> HTTP Stream

Wireshark · Follow HTTP Stream (tcp.stream eq 130) · Homework\_en.pcap

```
POST /processing/filedownload.php?id=loot HTTP/1.1
Host: www.filedropper.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.filedropper.com/loot
Cookie: __utma=231472648.769826256.1425493505.142549325.142549325.3;
__utms=231472648.1425493505.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none); __utmb=231472648;
514a1d63b5587=1519dc441350db5ca23ec2425c63eb76; __utmc=231472648
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 9

code=VPWRHTTP/1.1 200 OK
Date: Wed, 04 Mar 2015 19:08:59 GMT
Server: Apache
X-Powered-By: PHP/5.3.27
Content-Description: File Transfer
Content-Disposition: attachment; filename="loot.rar"
Content-Transfer-Encoding: binary
Expires: 0
Cache-Control: must-revalidate, post-check=0, pre-check=0
Pragma: public
Connection: close
Transfer-Encoding: chunked
Content-Type: application/octet-stream

Rar!.....S...
.....+.XF...@S.#<.[...]..B.v.e.L.vc/...rk...mZ.j..@..Z.L...#...".o.u#.....!..~M.S...oPaQ....h.j..w$
~..a-A..?.....U..S...&..q...Y...g...D..X>
.H.....)x.....U/-..(,v..L..)S.;U..3...;..Y!..uM..s...+.XF...".u..V...%.5.
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (1,352 bytes)

Show data as ASCII

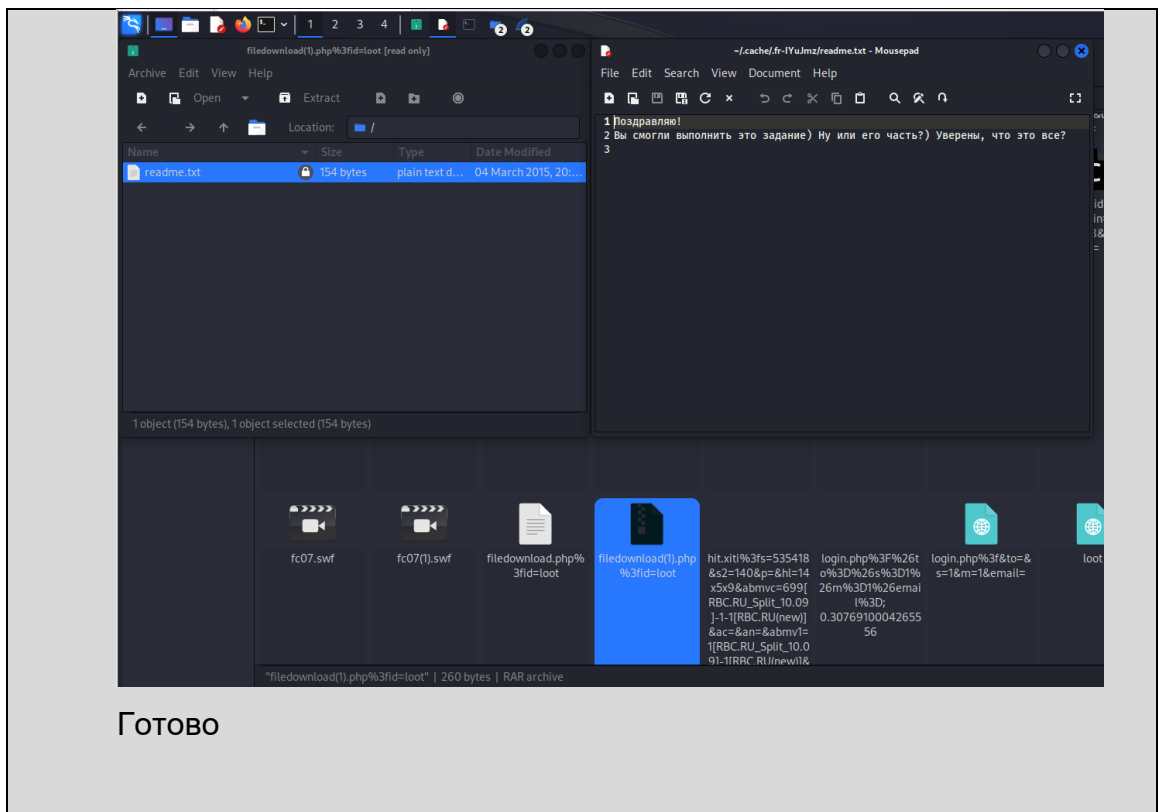
Find:

Filter Out This Stream Print Save as... Back Close

Видно, что этот rar-архив.

10. Скачаю его

File -> Export Objects -> HTTP -> Save all -> Нашёл нужный файл и  
всего скачанного. Ввёл пароль и открыл вложение



3. Ознакомиться со статьями 28, 272, 273, 274 Уголовного кодекса по ссылке «УК с комментариями» в «Дополнительных материалах». Грань между легальным и нелегальным применением инструментов очень тонкая.

Ознакомился