Задания заключительного этапа олимпиады «Я - профессионал» по направлению «Информационная и кибербезопасность»

Категория «Бакалавриат»

Задание 1 (12)

Для открытия банковской ячейки используется схема разделения секрета Блекли. Искомым ключом для банковской ячейки является решение системы уравнений по модулю простого числа. Ключ может быть восстановлен только при взаимодействии трех частей ключа (трех уравнений). Две принадлежат менеджерам банка и одна часть клиенту, которому необходимо предоставить доступ к ячейке. Найдите сумму трех координат ($(x_1 + x_2 + x_3)\ mod\ 17$) ключа, если известно, что клиенту было выдано уравнение:

$3x_1 + 4x_2 + 5x_3 = 3,$

а менеджеры банка владели частями ключами (уравнениями)

$2x_1 + 8x_2 + 11x_3 = 5,$

$x_1 + 13x_2 + 6x_3 = 12,$

все вычисления производятся по модулю простого числа p=17

Формат ответа: число

Решение:

Нужно решить систему уравнений относительно 3 переменных любым удобным способом, например, методом Гаусса:

$$\begin{cases} 3x_1 + 4x_2 + 5x_3 = 3\ (mod\ 17) \\ 2x_1 + 8x_2 + 11x_3 = 5\ (mod\ 17) \\ x_1 + 13x_2 + 6x_3 = 12\ (mod\ 17) \end{cases}$$

$$\begin{pmatrix} 3 & 4 & 5 & 3 \\ 2 & 8 & 11 & 5 \\ 1 & 13 & 6 & 12 \end{pmatrix} = \begin{pmatrix} 1 & 13 & 6 & 12 \\ 3 & 4 & 5 & 3 \\ 2 & 8 & 11 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 13 & 6 & 12 \\ 0 & -35 & -13 & -33 \\ 0 & -18 & -1 & -19 \end{pmatrix} = \begin{pmatrix} 1 & 13 & 6 & 12 \\ 0 & 16 & 4 & 1 \\ 0 & 16 & 16 & 15 \end{pmatrix} = \begin{pmatrix} 1 & 13 & 6 & 12 \\ 0 & 16 & 4 & 1 \\ 0 & 0 & 12 & 14 \end{pmatrix}$$

1) $x_3 = 14 * 12^{-1}\ mod\ 17 = 14 * 10 = 140\ (mod\ 17) = 4\ (mod\ 17)$
2) $16x_2 + 4 * 4 = 1\ (mod\ 17)$
   $16x_2 = -15\ (mod\ 17),$
   $x_2 = 2 * 16^{-1}\ (mod\ 17),$
   $x_2 = 2 * 16\ (mod\ 17) = 32\ mod\ 17 = 15,$
3) $x_1 + 13 * 15 + 6 * 4 = 12\ (mod\ 17)$
   $x_1 + 8 + 7 = 12\ (mod\ 17),$
   $x_1 = 14\ mod\ 17,$

$x_1 = 14, x_2 = 15, x_3 = 4$

$x_1 + x_2 + x_3 \; mod \; 17 = 14 + 15 + 4 \; mod \; 17 = 33 \; mod \; 17 = 16,$

Ответ: 16

Задание 2 (14)

Известно, что в классической (двоичной) ранцевой криптосистеме Меркла — Хеллмана для шифрации двоичного блока используется сверхвозрастающая последовательность из n целых чисел. То есть если n=10 и первое число в секретном ключе равно 11, то наименьшее возможное значение последнего (десятого) числа в секретном ключе будет 28016. Каким будет наименьшее возможное значение последнего (шестого) числа в секретном ключе в семиричной ранцевой криптосистеме Меркла — Хеллмана для n=6 и первого числа в секретном ключе равного 8?

Формат ответа: число

Решение

8, 8·6+1=49, (8+49)·6+1=49·7=343, 8·6+49·6 +343·6+1=343·7=2401, 8·6+49·6 +343·6 +2401·6 +1 = 2401·7=16807 , 8·6+49·6 +343·6 +2401·6 +2401·6 +16807·6 +1=16807·7=117649

Ответ: 117649

Задание 3 (20)

Задан многочлен f(x) є F_2[x]. Определить алгоритм, по которому многочлен F_2[x] раскладывается на многочлены, и определить эти многочлены.

f(x) = x^19 + x^16 + x^14 + x^11 + x^9 + x^8 + x^7 + x^5 + 1.

Формат ответа: 1. Алгоритм вида f(x)= 2. Многочлены

Решение

Определяем наличие кратных сомножителей. Для этого вычисляем формальную производную от f(x).

f’(x) = x^18 + x^10 + x^8 + x^6+ x^4 =x^4(x^14+x^6+x^4 +x^2+1) = x^4(x^7+x^3+x^2 +x+1)^2

Теперь используя алгоритм Евклида находим наибольший общий делитель для f(x) и f’(x)

g(x)=НОД(f(x), f’(x))= (x^7+x^3+x^2 +x+1)^2

f(x)/g(x) = (x^19 + x^16 + x^14 + x^11 + x^9 + x^8 + x^7 + x^5 + 1)/(x^14+x^6+x^4 +x^2+1)= x^5 +x^2+1.

Ответ: f1(x)= x^5 +x^2+1; f2(x)= x^7 + x^3+x^2+x+1; f(x)=f1(x)*f2(x)^2

Ответ: 1. f(x)=f1(x)*f2(x)^2

2. f1(x)= x^5 +x^2+1; f2(x)= x^7 + x^3+x^2+x+1;

Задание 4 (13)

Проинспектируйте в предложенном дампе трафика зашифрованную передачу и прочитайте файл с флагом внутри.

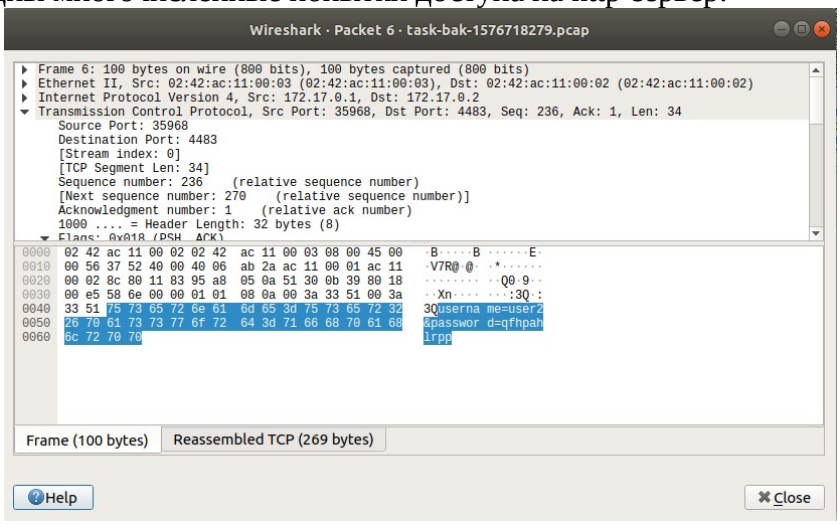
Чтобы получить файлы для этого задания, откройте архив *task4.7z* (пароль: `P@ssw0rdPr0tected`) на рабочем столе ВМ.

Формат ответа: flag{…}

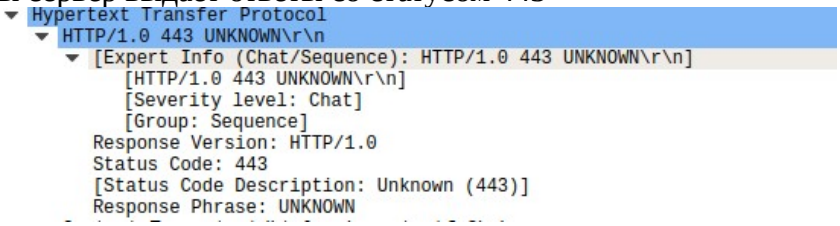
Ответ: flag{6f99765d445647e08f0a56f442515aa9}

Решение

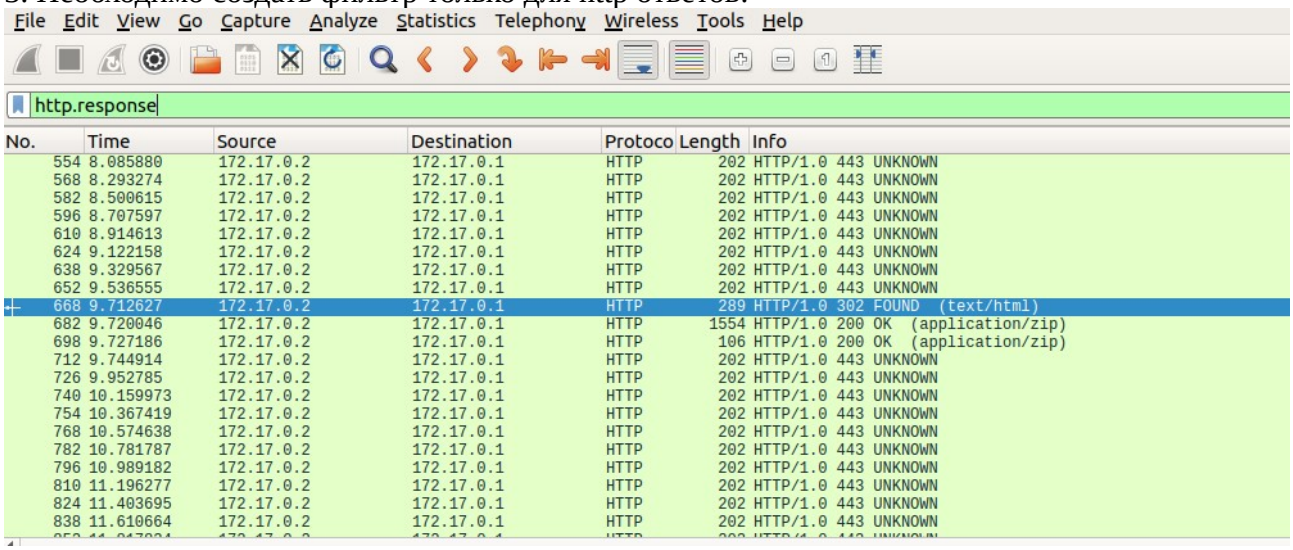
1. В трафике видны многочисленные попытки доступа на http сервер:



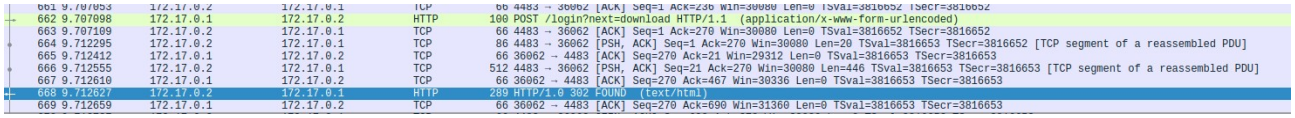
2. На эти запросы сервер выдает ответы со статусом 443

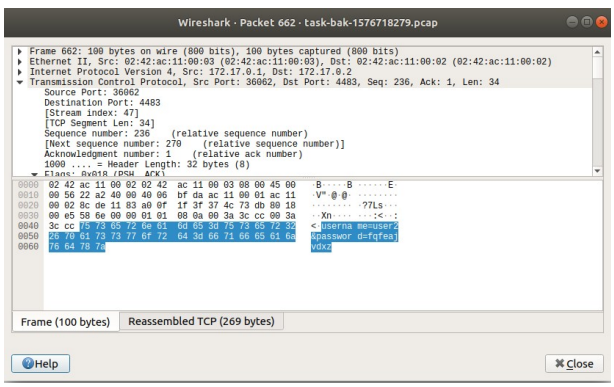


3. Необходимо создать фильтр только для http ответов:



4. Видно, что на один из запросов был получен отличный от обычного ответ со статусом 302. Необходимо проследовать по этому пакету и выше найти исходный запрос с логином и паролем (user2 fqfeajvdxz):

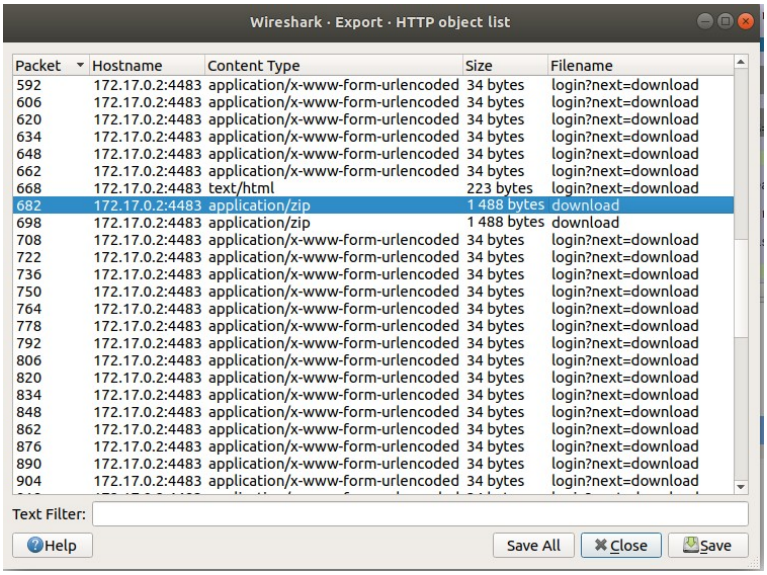




5. Далее происходит скачивание файла с именем key.zip:

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.0 200 OK\r\n
    ▼ [Expert Info (Chat/Sequence): HTTP/1.0 200 OK\r\n]
        [HTTP/1.0 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.0
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Content-Disposition: attachment; filename=key.zip\r\n
  ▶ Content-Length: 1488\r\n
    Content-Type: application/zip\r\n
    Last-Modified: Thu, 19 Dec 2019 00:52:36 GMT\r\n
    Cache-Control: public, max-age=43200\r\n
    Expires: Thu, 19 Dec 2019 13:18:27 GMT\r\n
    ETag: "1576716756.1256826-1488-469107834"\r\n
    Vary: Cookie\r\n
    Server: Werkzeug/0.16.0 Python/3.6.9\r\n
    Date: Thu, 19 Dec 2019 01:18:27 GMT\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.003580000 seconds]
    [Request in frame: 676]
    [Request URI: http://172.17.0.2:4483/download]
```

6. Этот файл можно можно сохранить отдельно при помощи пункта меню Export objects в wireshark.



Packet	Hostname	Content Type	Size	Filename
592	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
606	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
620	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
634	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
648	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
662	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
668	172.17.0.2:4483	text/html	223 bytes	login?next=download
682	172.17.0.2:4483	application/zip	1 488 bytes	download
698	172.17.0.2:4483	application/zip	1 488 bytes	download
708	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
722	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
736	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
750	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
764	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
778	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
792	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
806	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
820	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
834	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
848	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
862	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
876	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
890	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download
904	172.17.0.2:4483	application/x-www-form-urlencoded	34 bytes	login?next=download

7. Далее проверить его тип и удостовериться, что он имеет формат zip.

```
>file /tmp/download
/tmp/download: Zip archive data, at least v2.0 to extract
```

8. Затем его разархивировать, при запросе пароля указав пароль из пункта 4.

```
>unzip /tmp/download
Archive:  /tmp/download
[/tmp/download] server.key password:
```

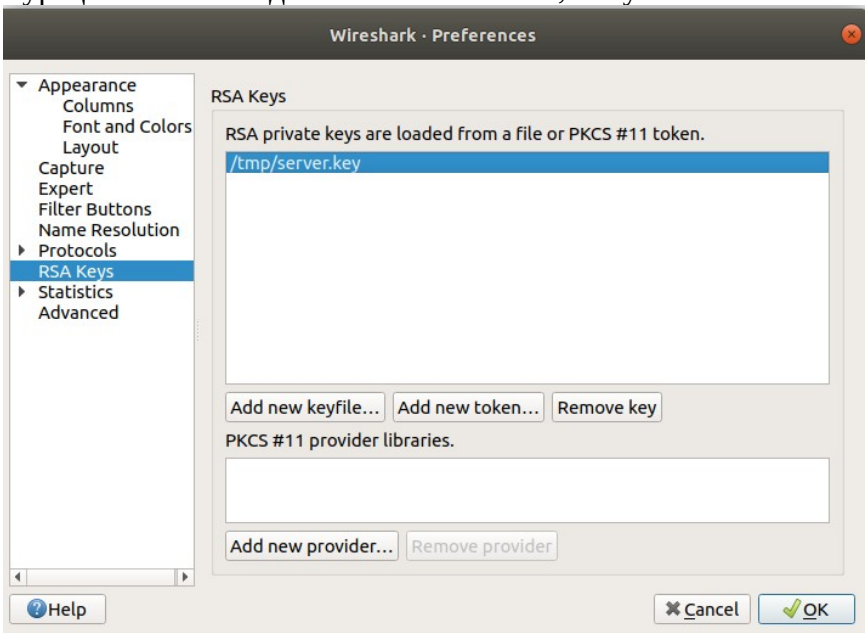
9. Разархивированный файл является ключом:

```
>unzip /tmp/download
Archive:  /tmp/download
[/tmp/download] server.key password:
  inflating: server.key
>file server.key
server.key: PEM RSA private key
```

10. Далее в дампе видим передачу по протоколу HTTPS:

998	14.028924	172.17.0.2	172.17.0.1	TCP	74	443 → 44312 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3817732 TSecr=3817732 WS=128
999	14.028978	172.17.0.1	172.17.0.2	TCP	66	44312 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3817732 TSecr=3817732
1000	14.029529	172.17.0.1	172.17.0.2	TLSv1.2	359	Client Hello
1001	14.029551	172.17.0.2	172.17.0.1	TCP	66	443 → 44312 [ACK] Seq=1 Ack=294 Win=30080 Len=0 TSval=3817733 TSecr=3817733
1002	14.029797	172.17.0.2	172.17.0.1	TLSv1.2	1081	Server Hello, Certificate, Server Hello Done
1003	14.029833	172.17.0.1	172.17.0.2	TCP	66	44312 → 443 [ACK] Seq=294 Ack=1016 Win=31232 Len=0 TSval=3817733 TSecr=3817733
1004	14.030401	172.17.0.1	172.17.0.2	TLSv1.2	384	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1005	14.033969	172.17.0.2	172.17.0.1	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1006	14.034224	172.17.0.1	172.17.0.2	TLSv1.2	236	Application Data
1007	14.034459	172.17.0.2	172.17.0.1	TLSv1.2	394	Application Data

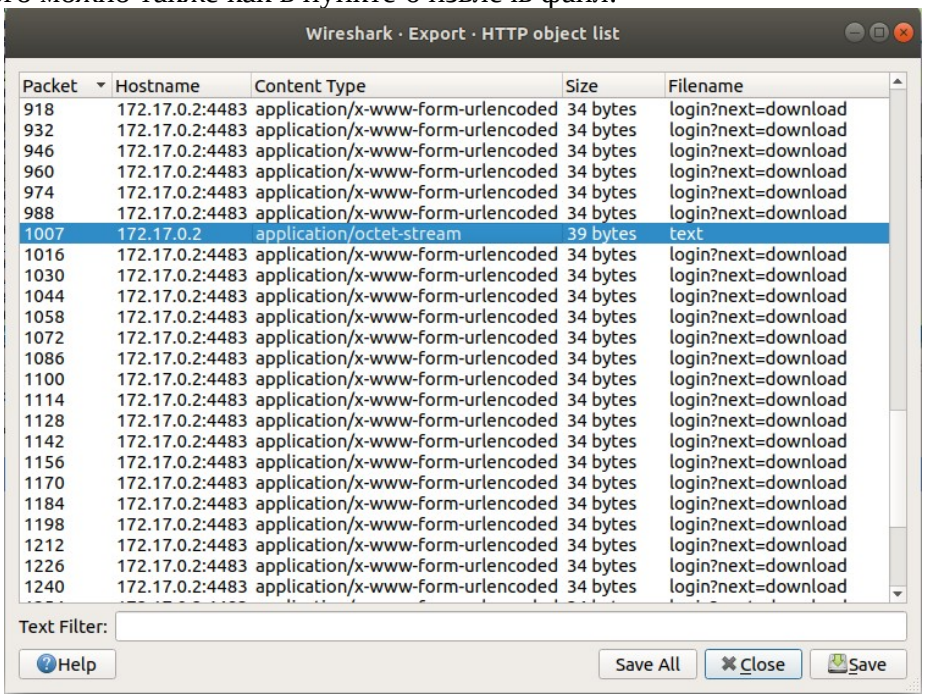
11. Через конфигурацию wireshark добавляем RSA ключ, полученный на этапе 9:



12. После этого wireshark автоматически расшифровывает трафик при помощи указанного ключа и показывает уже в открытом виде:

1000	14.029529	172.17.0.1	172.17.0.2	TLSv1.2	359	Client Hello
1001	14.029551	172.17.0.2	172.17.0.1	TCP	66	443 → 44312 [ACK] Seq=1 Ack=294 Win=30080 Len=0 TSval=3817733 TSecr=3817733
1002	14.029797	172.17.0.2	172.17.0.1	TLSv1.2	1081	Server Hello, Certificate, Server Hello Done
1003	14.029833	172.17.0.1	172.17.0.2	TCP	66	44312 → 443 [ACK] Seq=294 Ack=1016 Win=31232 Len=0 TSval=3817733 TSecr=3817733
1004	14.030401	172.17.0.1	172.17.0.2	TLSv1.2	384	Client Key Exchange, Change Cipher Spec, Finished
1005	14.033969	172.17.0.2	172.17.0.1	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Finished
1006	14.034224	172.17.0.1	172.17.0.2	HTTP	236	GET /text HTTP/1.1
1007	14.034459	172.17.0.2	172.17.0.1	HTTP	394	HTTP/1.1 200 OK

13. После этого можно также как в пункте 6 извлечь файл:



14. Открыв его, узнаем ответ на задание:

```
>cat /tmp/text
flag{6f99765d445647e08f0a56f442515aa9}
```

Задание 5 (16)

Network Forensics — Piligrim

Задание подготовлено сообществом SPbCTF (vk.com/spbctf)

ФСБ ликует: мессенджер Piligrim наконец предоставил им ключи шифрования. Ключи подошли, в файле PILIGRIM_20200109001337_20200109001347.decrypted.pcap расшифрованный трафик. Однако сообщений слишком много, штатные сотрудники не справляются.

Ваша задача — найти сообщение с секретным флагом. Похожих сообщений много, но секретное единственное, которое отправлено на сервер, но ещё никем не получено.

Чтобы получить файлы для этого задания, откройте архив tasks_archive_bachelor.7z (пароль: `adaptive39stayed`) на рабочем столе ВМ. Искомые файлы внутри директории `forensics_ez_piligrim/`.

Формат ответа: yaprofi{...}

Решение

В трафике запись сессий WebSocket. Вебсокет интересен тем, что ответы от сервера видны в трафике в сыром виде, а запросы клиента «маскируются» — шифруются коротким ксором, поэтому их впрямую не видно.

С помощью Wireshark выдерем все отправленные сообщения:

```
tshark -r PILIGRIM_20200109001337_20200109001347.decrypted.pcap -Tfields -etext | grep '"action":"send"' > allsend.txt
```

Выдерем все полученные сообщения:

```
tshark -r PILIGRIM_20200109001337_20200109001347.decrypted.pcap -Tfields -etext | grep '"sender"' > allrecv.txt
```

Вычтем множества — оставим те, которые есть в отправленных, но нет в полученных:

```
(grep -Po '"message":"[^"]*"' allsend.txt ; grep -Po '"message":"[^"]*"' allrecv.txt) | sort | uniq -u
```

"message":"i heard that SPbCTF loves different challenges: vk.com/spbctf"

"message":"i heard that this task was made by Vlad Roskov"

"message":"i heard the flag is yaprofi{b39c0858661a72fa91cdf505644eced5}"

Ответ: yaprofi{b39c0858661a72fa91cdf505644eced5}

Задание 6 (25)

Crypto Medium — Linear

Задание подготовлено сообществом SPbCTF (vk.com/spbctf)

Вам дана программа, осуществляющая процедуру шифрования выбранного текста.

python3 encrypt.py MESSAGE

Программа принимает на вход сообщение, генерирует приватный ключ и выводит результат шифрования на экран в виде набора чисел.

Удалось перехватить результаты зашифрования пяти сообщений на одном и том же ключе:

1. CRYPT: -12211 -15753 -6429 17625 15441

2. FLASH: -9595 -15633 -7782 16131 14658

3. OLYMP: -12215 -16648 -6287 16834 15877

4. FORTH: -11085 -15428 -6201 16608 15819

5. TODAY: -10085 -16959 -9114 16835 13485

Расшифруйте искомое сообщение, зашифрованное на том же самом ключе, что и пятерка, приведенных выше.

-11130 -15712 -5883 16392 16358

Чтобы получить файлы для этого задания, откройте архив *tasks_archive_bachelor.7z* (пароль: `adaptive39stayed`) на рабочем столе ВМ. Искомые файлы внутри директории `crypto_md_linear/`.

Формат ответа: осмысленный текст

Ответ: MOUSE

Решение

Авторское решение представлено по ссылке: https://gist.github.com/v0s/e52dcaad8bd248323dd19e3c78e27fbf

yaprofessional

Alexander Menshchikov (n0str)

November 2019

1 Encryption

Secret text (bytes): [1, 3]

Secret key (in matrix form): K = $\begin{pmatrix} 2 & 1 \\ 2 & -1 \end{pmatrix}$

Multiply message to key:

$$k_{11}s_1 + k_{12}s_2 = c_1$$
$$k_{21}s_1 + k_{22}s_2 = c_2$$

Denote C = $\begin{pmatrix} c_1 & c_2 \end{pmatrix}$ as ciphertext.
Solving

$$2 * 1 + 1 * 3 = 5$$
$$2 * 1 - 1 * 3 = -1$$

Produces: C = $\begin{pmatrix} 5 & -1 \end{pmatrix}$

2 Decryption

Given secret key and ciphertext.

Solve system of linear equations: $\begin{cases} 2x + y & = 5 \\ 2x - y & = -1 \end{cases}$

Where solution (x, y) = (1, 3) is a plaintext.

3 Task

Student gets ciphertext C = $\begin{pmatrix} c_1 & c_2 & ... & c_n \end{pmatrix}$ and N pairs of plaintext and ciphertext (on shared key). He should restore key matrix and decrypt secret message.

4 Example

S = $\begin{pmatrix} 5 & -1 \end{pmatrix}$,
$P_1 = \begin{pmatrix} 3 & 5 \end{pmatrix}$,
$P_2 = \begin{pmatrix} 2 & -1 \end{pmatrix}$,

$C_1 = \begin{pmatrix} 11 & 1 \end{pmatrix}$,
$C_2 = \begin{pmatrix} 3 & 4 \end{pmatrix}$

There are two systems: $\begin{cases} \mathrm{k}_{11} * 3 + k_{12} * 5 & = 11 \\ k_{21} * 3 + k_{22} * 5 & = 1 \end{cases}$

and $\begin{cases} \mathrm{k}_{11} * 2 - k_{12} & = 3 \\ k_{21} * 2 - k_{22} & = 5 \end{cases}$

Can be rewritten as: $\begin{cases} \mathrm{k}_{11} * 3 + k_{12} * 5 & = 11 \\ k_{11} * 2 - k_{12} & = 3 \end{cases}$

and $\begin{cases} \mathrm{k}_{21} * 3 + k_{22} * 5 & = 1 \\ k_{21} * 2 - k_{22} & = 5 \end{cases}$

Solving these equations gives $k_{11} = 2, k_{12} = 1, k_{21} = 2, k_{22} = -1$

Now we have a key matrix K $= \begin{pmatrix} 2 & 1 \\ 2 & -1 \end{pmatrix}$ and can solve the following system to obtain secret message: $\begin{cases} 2S_1 + S_2 & = 5 \\ 2S_1 - S_2 & = -1 \end{cases}$

So, $S_1 = 1, S_2 = 3$

5 Source code

https://gist.github.com/n0str/e52505f3790c380587f100cc5303e7e8