



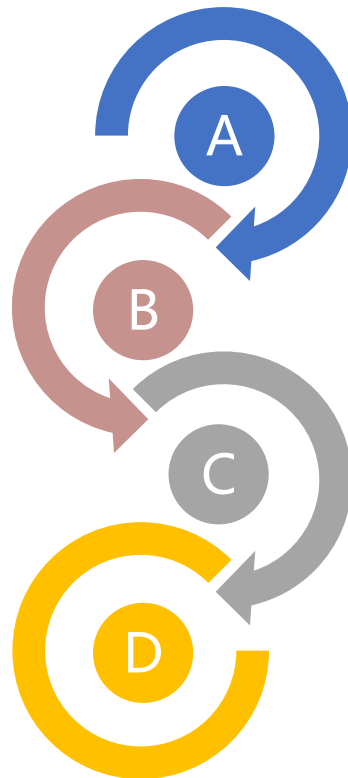
# Про безопасность

От команды [LIFE] Sudo Su

# Что мы будем обсуждать?

Какие есть соревнования

Вопросы, выводы и  
страхи



Почему ИБ  
важно?

Небольшая  
история

# Почему ИБ важно?

В этом году:

-> В сеть сливают данные о клиентах:

-> (6 июня):

Ашан - 7,840,297 (клиентов)

Аптека низких цен - 98,578 (заказов)

Gloria Jeans - 2,36 млн уникальных мобильных номеров

-> (7 июня):

book24.ru – 4,003,488 (клиентов)

askona.ru – 1,948,828 (клиентов)

-> (8 июня):


Буквоед – 3,580,578 (клиентов)

Леруа Мерлен – 1,750,227 (клиентов)

ТВОЕ – 2,268,634 (клиентов)

-> (10 июня): Читай-город – 9,800,830 (клиентов)

(и так далее...)



## Почему ИБ важно?

last_name	middle_name	phone	email	created_at	updated_at
	Борисович	+726047	super-admin@auchan-ecom.ru	2020-04-13 21:12:12	2020-04-13 21:12:12
	Максимович	+733622	admin@auchan-ecom.ru	2020-04-13 21:12:12	2020-04-13 21:12:12
	Покупатель	+791111	customer@test.ru	2020-04-17 21:35:10	2020-04-17 21:35:10
	Покупатель	+797777	customer2@test.ru	2020-04-20 10:02:32	2020-04-20 10:02:32
	Тестович	+799999	testshop@auchan-ecom.ru	2020-04-22 21:33:16	2020-04-22 21:33:16
	NULL	+978712	e@gmail.com	2020-05-07 09:35:29	2021-02-13 04:38:22
	NULL	+790320	@auchan.ru	2020-05-07 10:40:03	2022-07-23 19:41:52
	NULL	+792618	.null@gmail.com	2020-05-07 11:36:55	2020-05-07 11:36:55
	NULL	+796362	elov@auchan.ru	2020-05-07 19:50:00	2021-02-13 04:38:22

"tel":"(800)-60"email":"dop":"Заказ от страховой компании INSUR.ANCTM.BIZ (API)"	"summ":205.27	"date":"18.05.2023	"apt":"ул. Пушкина
"tel":"(063)448"email":"dop":"" INSUR.ANCTM.BIZ"	"summ":108.54	"date":"18.05.2023	"apt":"пр. Вячеслава Черновола
"tel":"(096)170"email":"dop":"Заказ от страховой компании INSUR.ANCTM.BIZ (API)"	"summ":75.7	"date":"18.05.2023	"apt":"ул. Гоголя
"tel":"(800)-60"email":"dop":"Заказ от страховой компании INSUR.ANCTM.BIZ (API)"	"summ":821.79	"date":"18.05.2023	"apt":"ул. Княжий затон
"tel":"(095)281"email":"dop":"Заказ от страховой компании INSUR.ANCTM.BIZ (API)"	"summ":200.4	"date":"18.05.2023	"apt":"ул. Семена Паля
"tel":"(096)170"email":"dop":"Заказ от страховой компании INSUR.ANCTM.BIZ (API)"	"summ":204.3	"date":"18.05.2023	"apt":"ул. Одесская
"tel":"(095)753"email":"dop":"" INSUR.ANCTM.BIZ"	"summ":816.94	"date":"18.05.2023	"apt":"ул. Центральная
"tel":"(096)170"email":"dop":"Заказ от страховой компании INSUR.ANCTM.BIZ (API)"	"summ":127.8	"date":"18.05.2023	"apt":"ул. Соборная
"tel":"(096)170"email":"dop":"Заказ от страховой компании INSUR.ANCTM.BIZ (API)"	"summ":1131.98	"date":"18.05.2023	"apt":"ул. Центральная
"tel":"(096)170"email":"dop":"Заказ от страховой компании INSUR.ANCTM.BIZ (API)"	"summ":208.2	"date":"18.05.2023	"apt":"Героев Труда ул.



## Почему ИБ важно?

icuserid	ccusfullname	ccusinn	ccitizenship	cgender	dbirthdate	cmainphonenum
939084	КУДИНОВ ВЛАДИМИР ГЕННАДЬЕВИЧ	"263507934871"	РОССИЯ	M	1955-11-28	+79887415988↓
939085	ЗАРИПОВ АЙДАР ВИЛЕВИЧ	"026906996112"	РОССИЯ	M	1980-07-14	+79107046760↓
939086	ИВАШКИН АНДРЕЙ ВЛАДИСЛАВОВИЧ	"434561714833"	РОССИЯ	M	1969-12-30	+79634327169↓
939087	КУРУШИНА МАРИЯ АЛЕКСЕЕВНА	"370226063260"	РОССИЯ	F	1999-07-06	+79109847298↓
939088	КУРКИН СЕРГЕЙ АЛЕКСЕЕВИЧ	"545261447803"	РОССИЯ	M	1963-09-06	+79118637107↓
939089	КЛИМЕНКО ВИКТОРИЯ ВИКТОРОВНА	"262411658604"	РОССИЯ	F	1993-09-11	+79187566131↓
939090	ИВАНЕНКО ОЛЬГА НИКОЛАЕВНА	"781660107577"	РОССИЯ	F	1977-02-22	+79657890269↓
939091	МУКАЕВ МАВЛЮТ МУГАЛИМОВИЧ	"020703579218"	РОССИЯ	M	1958-09-28	+79177339009↓
939092	ЩИРОВА ГАЛИНА ВЛАДИМИРОВНА	"771910374934"	РОССИЯ	F	1955-12-26	+79850891404↓
939093	ШОЕВ СУЛАЙМОН АНВАРХОДЖАЕВИЧ	"165121547870"	РОССИЯ	M	1986-10-04	+79874195636↓
939094	РАЙХЕРТ ЛИЛИЯ РОБЕРТОВНА	"550111326349"	РОССИЯ	F	1979-09-18	+79139666149↓
939095	ФИЛИПPOB ДМИТРИЙ ИВАНОВИЧ	"020901524570"	РОССИЯ	M	1987-02-24	+79297559472↓
939096	БОЛЬШАКОВА ИРИНА НИКОЛАЕВНА	"631813832820"	РОССИЯ	F	1963-03-31	+79277640084↓
939097	ФОМИН ВЛАДИСЛАВ ЛЕОНИДОВИЧ	"507206450433"	РОССИЯ	M	1999-05-19	+79855696022↓
939098	АНДРЕЕВ ДМИТРИЙ ВЛАДИМИРОВИЧ	"270603446821"	РОССИЯ	M	1992-12-18	+79144028821↓
939099	КРАЕВ ГЛЕБ ЛЕОНИДОВИЧ	"631629155800"	РОССИЯ	M	1986-04-29	+79608199918↓
939100	ТЮМНЕВ АЛЕКСАНДР ВАЛЕРЬЕВИЧ	"504017719725"	РОССИЯ	M	1990-10-04	+79688224747↓
939101	КОРАБЕЛЬ АРТЕМ АЛЕКСАНДРОВИЧ	"531901654148"	РОССИЯ	M	1988-08-04	+79506819674↓
939102	КОЖИН СЕРГЕЙ ВЯЧЕСЛАВОВИЧ	"231100105211"	РОССИЯ	M	1971-12-23	+79892669635↓
939103	ТКАЧЕВА ЕЛЕНА АЛЕКСАНДРОВНА	"741707957263"	РОССИЯ	F	1976-08-12	+79000267537↓
939104	ШУЛЬГИНА ЕЛЕНА ВАЛЕРЬЕВНА	"720410089910"	РОССИЯ	F	1977-07-21	+79123852496↓
939105	САЙБЕЛЬ КРИСТИНА АНДРЕЕВНА	"230110087471"	РОССИЯ	F	1985-07-13	+79184986037↓
939106	НЯГУ АЛЕКСАНДР ГЕОРГИЕВИЧ	"614807733430"	РОССИЯ	M	1984-11-19	+79150903385↓
939107	ПЕТРОВА ЕЛЕНА ВИТАЛЬЕВНА	"860100769706"	РОССИЯ	F	1975-06-30	+79105603029↓
939108	ПЯТКОВСКАЯ НАТАЛЬЯ ВАЛЕРЬЕВНА	"622502652348"	РОССИЯ	F	1981-11-14	+79109087510↓
939109	ЗАЙЦЕВА ОЛЬГА НИКОЛАЕВНА	"366509040500"	РОССИЯ	F	1974-05-18	+79855451272↓
939110	АЛЫЕВ АГИЛ ГАСАН ОГЛЫ	"672900297158"	РОССИЯ	M	1968-11-25	+79156494589↓
939111	КУЧЕР ОКСАНА ОЛЕГОВНА	"234605989984"	РОССИЯ	F	1991-06-09	+79280355300↓
939112	РЯБОВ ВЛАДИМИР НИКОЛАЕВИЧ	"225302233513"	РОССИЯ	M	1969-03-04	+79825707027↓
939113	ЦАРЬКОВ ДМИТРИЙ ИВАНОВИЧ	"332601433659"	РОССИЯ	M	1994-10-02	+79157767571↓

# Какие есть соревнования

-> CTF (task-based)

-> KoTH

-> A/D

-> Олимпиады

-> Хакатоны



## Какие есть соревнования (CTF(task-based))

admin — задачи на администрирование

pwn — эксплуатация уязвимостей

osint / recon — поиск информации в открытых источниках

forensic — компьютерно-криминалистическая экспертиза

joy — различные развлекательные задачи

reverse — исследование программ без исходного кода

stegano — стеганография

ppc — задачи на программирование

crypto — криптография

web — задачи на веб-уязвимости

ctb — задачи на аудит удалённых машин

misc — сборник

network - знание сетевой инфраструктуры и протоколов

juristic — знание законодательства



## Какие есть соревнования (CTF(task-based))

Admin дурак, а модератор то ещё отребье

Задача: Найти в архиве с 1000 папками флаг. (Схожая с Polygon CTF)

Подключиться к серверу и найти какие-то файлы. Настройка сервера и схожие задачи с управлением сервера и процессов -> Всё это в данной категории.

Что знать?

База:

- Как работает Windows, Linux, какие команды есть, что и как включать/отключать
- Уметь печатать на клавиатуре, как ковбой
- Любить теперь LIFE





# Какие есть соревнования (CTF(task-based))

## Reverse (Как достать программу 1)

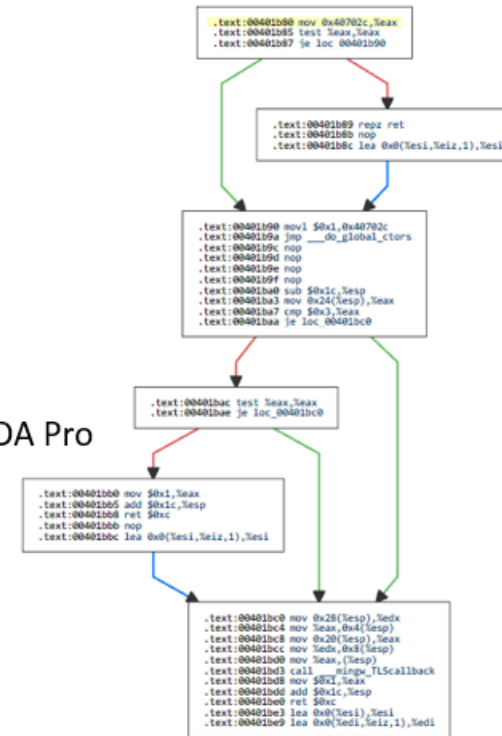
Задача: Изучить программу и получить флаг

Что знать?

База:

Знать +- Ассемблер, С. Работать с дебагерами по типу OlllyDebug или IDA Pro  
Уметь печатать на клавиатуре, как ковбой  
Да, снова любить LIFE

```
C:\Users\An1x\Desktop\эштхЕешЕхС\ёёюЕърЕшьр\example\main.exe
Write password:fs
Ещё что напишешь?
Write password: _
```



## Какие есть соревнования (CTF(task-based))

### pwn

Нужно взламывать программы, которые вы запускаете у себя на телефоне, компьютере и прочее

Что знать:

- Как вообще машина запускает, компилирует и хранит программы

- Уметь реверсить

- И знать ассемблер



# Какие есть соревнования (CTF(task-based))

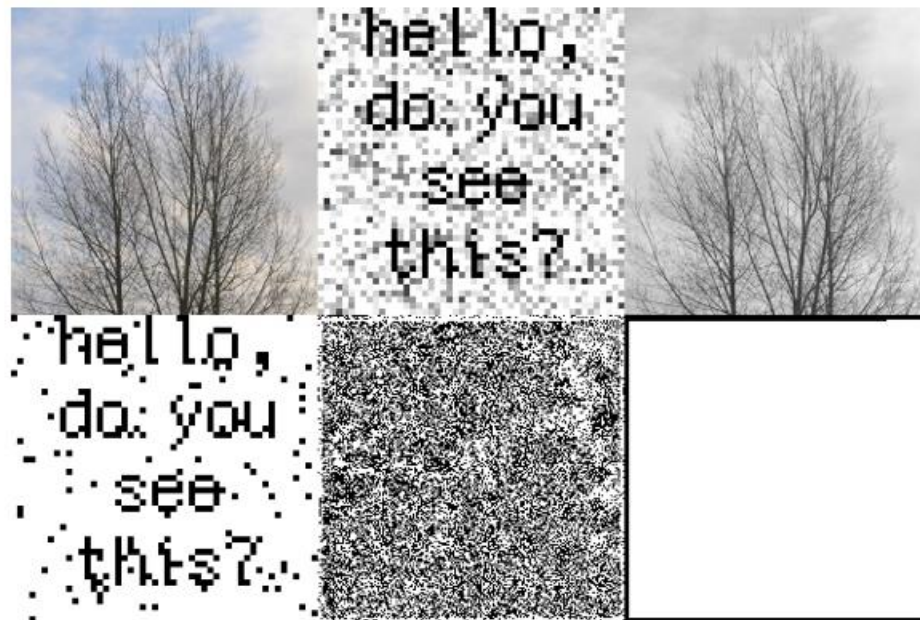
## Stegano (Бабка спрятала, а ты гадай 1)

Задача: Дан файл. Необходимо узнать, что в нём спрятано

Что знать?

База:

- Как работают форматы файлов
- Как скрывать данные в этих механизмах
- Уметь программировать на python | C++ | Java



Какие есть соревнования (**CTF**(task-based))

## Crypto (Бабка загадала, а ты думай)

Задача: Дан текст. Расшифруйте oujp{xkurpjcxah\_ljnbja\_lryqna}

Что знать?

База:

- Уметь программировать

- Знать методы шифрования и уметь их реализовывать на языках программирования

- Кодировки символов



# Какие есть соревнования (CTF(task-based))

## Web (Всё видно, только тыкни и сломай. Мы же богатые)

Задача: Есть сайт. Получите флаг

Что не надо знать?

База:

Уметь программировать

Досканально понимать, как и что работает на сайте

Искать в нём дыры

(Если продолжение будет, то веб буду я вести и всё расскажу)



```
1 <!doctype html>
2 <html>
3   <head>
4     <link rel="stylesheet" href="style.css" />
5     <script src="script.js"></script>
6   </head>
7   <body>
8     
9     <div></div>
10  </body>
11 </html>
12
13 <!-- flag part 1: flag{bd6a9e3f -->
14
```



# Какие есть соревнования (CTF(task-based))

## Forensics(Замарали ваш ёршик, а вы ищите, кто это)

Задача: Дан вам дамп памяти, а вы должны узнать пароль от учётной записи пользователя

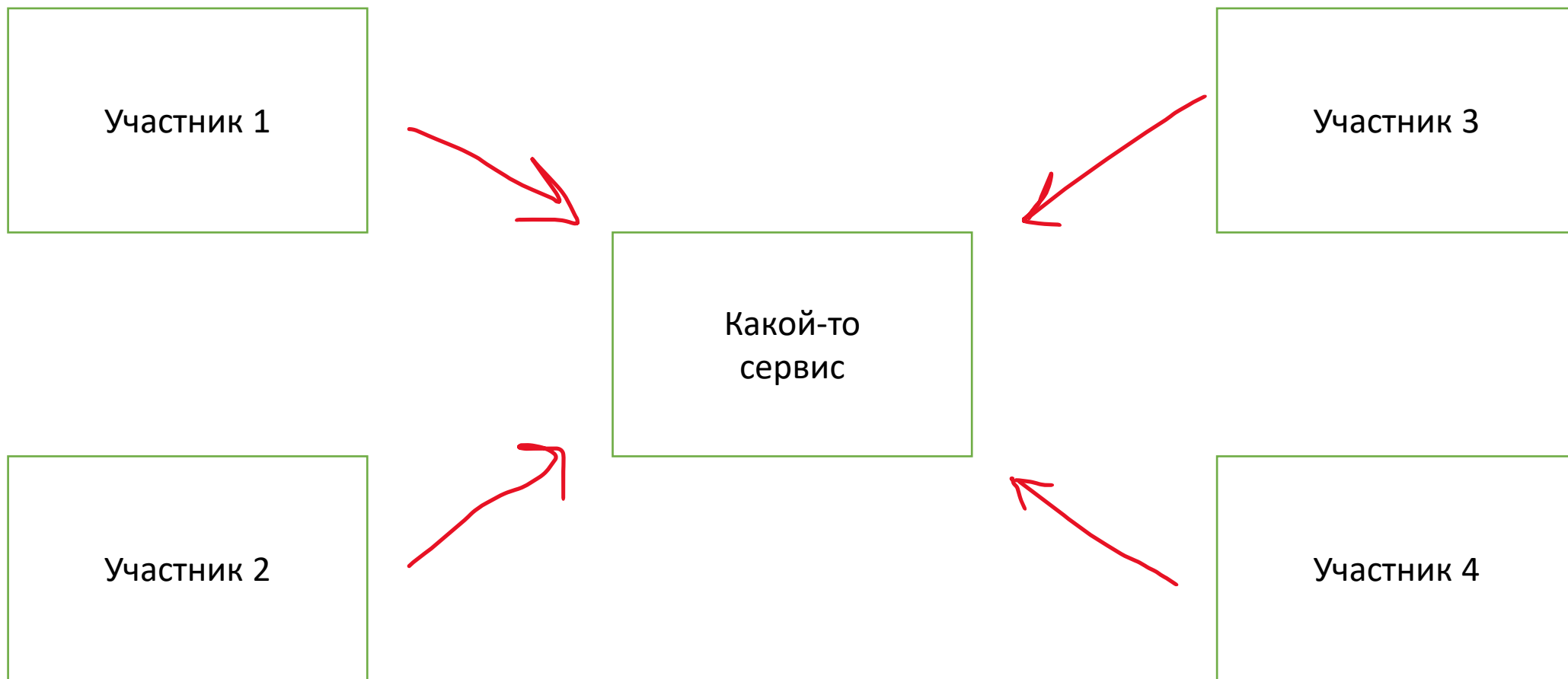
Что знать?

База:

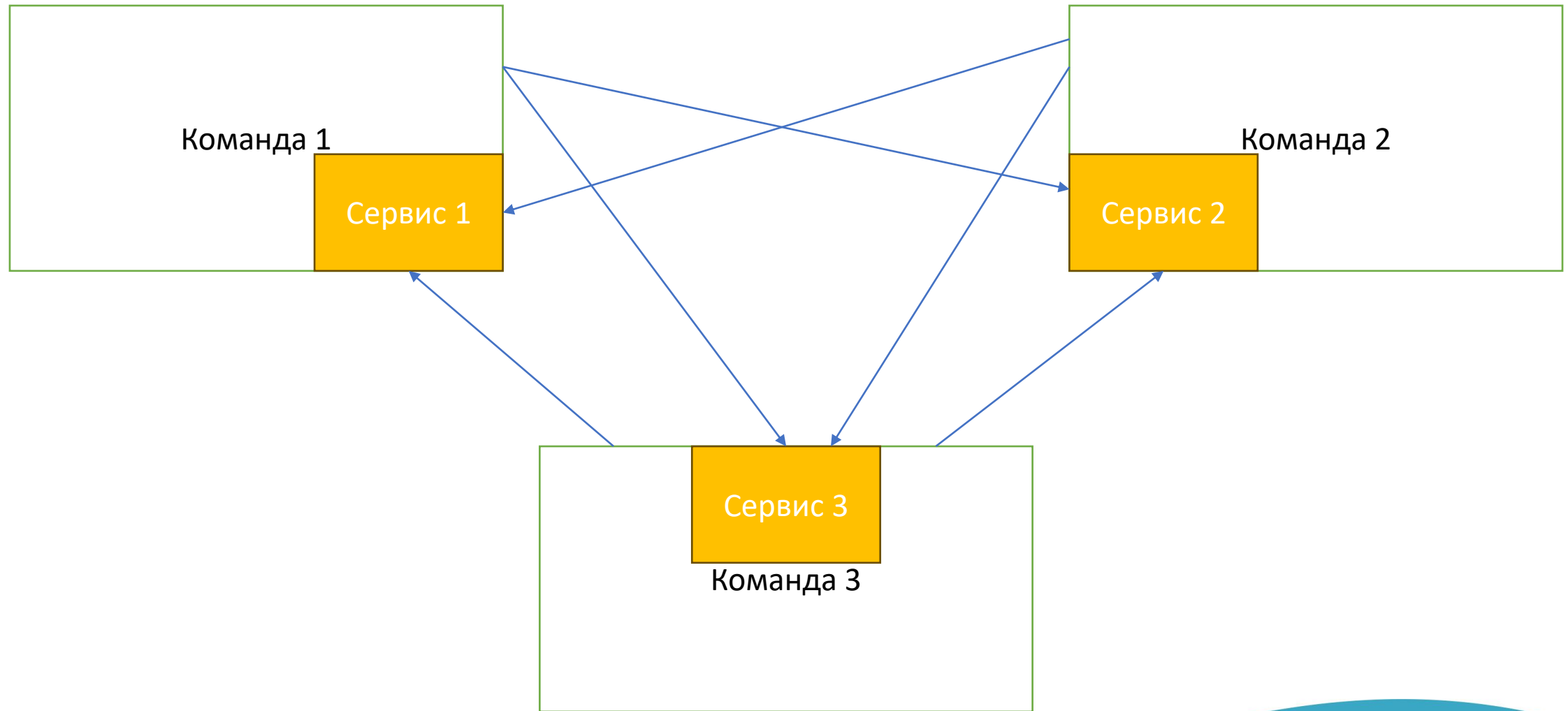
- Анализ процессов в ОС
- Средства дампа и их работа
- Работа с памятью компьютера
- (Да много чего, потом ещё уточним)

```
(root@kali-rdp)~/home/henry/writeup/pub
# /tmp/volatility/vol.py -f challenge.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win10x64_18362
                             AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                             AS Layer2 : FileAddressSpace (/home/henry/writeup/pub/challenge.vmem)
                             PAE type : No PAE
                             DTB : 0x1ad000L
                             KDBG : 0xf8047cadaa80L
      Number of Processors : 8
      Image Type (Service Pack) : 0
      KPCR for CPU 0 : 0xffffffff8047b803000L
      KPCR for CPU 1 : 0xffffffff802d9c0000L
      KPCR for CPU 2 : 0xffffffff802db86000L
      KPCR for CPU 3 : 0xffffffff802d5e2000L
      KPCR for CPU 4 : 0xffffffff802d8cb000L
      KPCR for CPU 5 : 0xffffffff802dcce000L
      KPCR for CPU 6 : 0xffffffff802dd79000L
      KPCR for CPU 7 : 0xffffffff802dde0000L
      KUSER_SHARED_DATA : 0xffffffff7800000000L
      Image date and time : 2021-01-18 13:51:49 UTC+0000
      Image local date and time : 2021-01-18 05:51:49 -0800
```

## Какие есть соревнования (KoTH)



## Какие есть соревнования (A/D)



# Какие есть соревнования (Олимпиады)

Ключ:

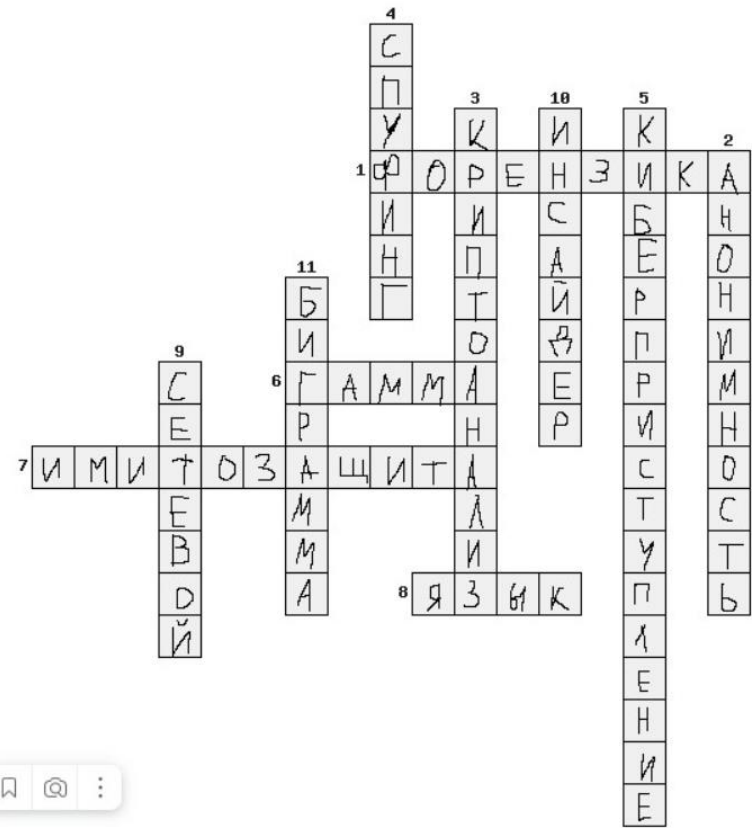
1 – 6, 10 – 4, 5 – 6, 10 – 8, 1 – 4, 3 – 5, 2 – 4, 8 – 3, 9 – 7, 4 – 2, 5 – 11, 2 – 12  
10 – 6, 5 – 9, 3 – 10, 7 – 7, 10 – 6, 2 – 3, 3 – 1, 3 – 1

Таблица:

Буква	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Код	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Буква	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	
Код	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
Буква	<	>	!	%													
Код	35	36	37	38													

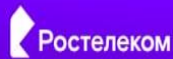
Сообщение для расшифровки:

4 36 12 31 7 36 34 14 19 35 18 27 34 32 18 17 20 25 24 9 15 14 16 5 18



## Какие есть соревнования (Хакатон)





### Безопасное видеонаблюдение

Разработать прототип системы контроля пропускного режима на удалённом складе.

[Подробнее](#)[Решить](#)

### Системы мониторинга и оперативного уведомления


Разработать прототип системы мониторинга оборудования и учета простоев

[Подробнее](#)[Решить](#)

### Определение местоположения БВС в условиях отсутствия GPS\ГЛОНАСС сигнала

Определить координаты борта  
Реализовать алгоритм прогнозирования местонахождения БВС

[Подробнее](#)[Решить](#)



### Обеспечение защиты данных

Осуществить защиту данных пользователя смартфона в процессе деловых коммуникаций

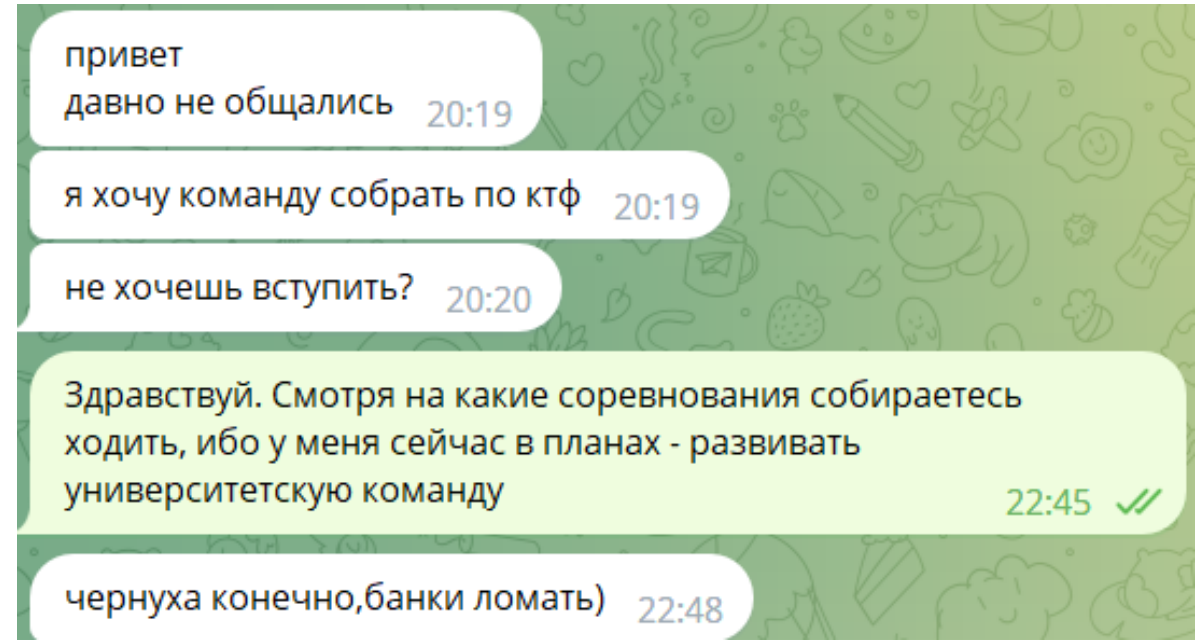
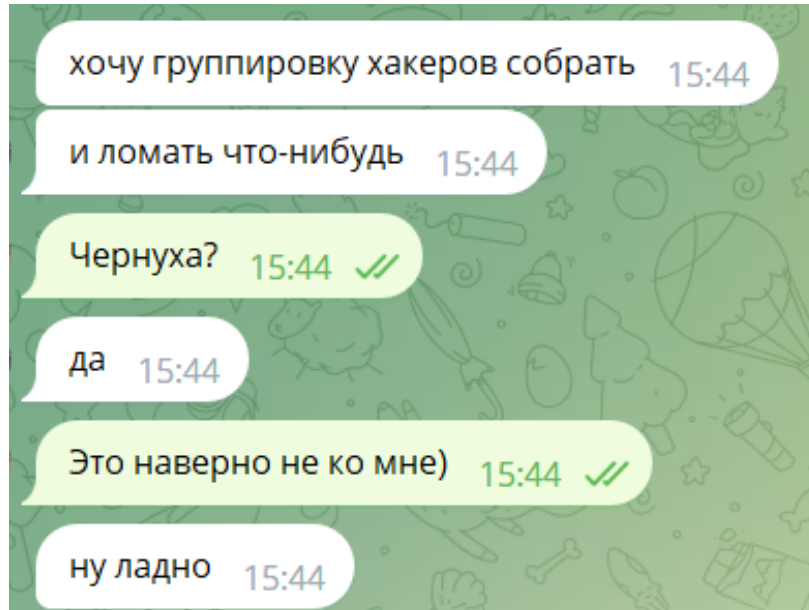
[Подробнее](#)[Решить](#)



# Немного истории



# Это мы осуждаем, и против этого боремся



НГС

<https://ngs.ru> > text > gorod > 2023/04/28

## Студент НГТУ взломал сайт и слил ответы на тесты

28 апр. 2023 г. — Студент Новосибирского государственного технического университета (НГТУ НЭТИ) Артем Асачьев взломал сайт университета и слил ответы н...



*Храни вас господь*

Выпускаем продолжение?



Наш чат во вконтакте



Наш чат во телеграмме



Как меня найти

