Министерство образования Республики Беларусь
Учреждение образования
“Гомельский государственный университет им. Франциска Скорины”

Отчёт по лабораторной работе №1

«Сбор предварительной информации»

Выполнил:
Студент группы МС-42
Шалюта А.Н.
Проверил:
Старший преподаватель
Грищенко В.В.

2022

Цель работы: Целью лабораторной работы является обучение методам и средствам сбора предварительной информации в Интернет об анализируемойКС.

Ход работы.

Шаг 1. Перейдём по адресу http://www.ripn.net/nic/whois. Укажем домен rmkk.by

rmkk.by

Updated 1 second ago

```
Domain name: rmkk.by
Registrar: Open Contact, Ltd
Org: ОАО "Рогачевский МКК"
Country: BY
Address: 247671, Гомельская, Рогачев, ул. Кирова, 31, 1
Registration or other identification number: 400046241
Phone: +3750233938390
Email: HIDDEN! Details are available at https://whois.cctld.by
Name Server: a1.domain.by
Name Server: a2.domain.by
Update Date: 2022-11-15
Creation Date: 2006-03-16
Expiration Date: 2024-03-22

-----------------------------------------
Service provided by Belarusian Cloud Technologies LLC
```

Результаты проверки домена rmkk.by

Информация о домене

Регистратор:

Открытый контакт
Open Contact, Ltd

Владелец домена:

ОАО "Рогачевский МКК"
BY, Рогачев, Гомельская, 247671, ул. Кирова, 31, 1
Регистрационный или иной идентификационный номер: 400046241
Телефон: +3750233938390
E-mail: asup@rmkk.by

DNS-серверы:

a1.domain.by
a2.domain.by

Состояние:

Дата создания: 2006-03-16
Дата последнего обновления: 2022-11-15
Дата окончания: 2024-03-23

Шаг 2. Перейдём по адресу https://network-tools.com/nslookup/ и зададимпараметры: домен – bsmu.by, тип запроса – ANY. Определим почтовый сервер организации.

name	class	type	data	time to live
rmkk.by	IN	A	195.50.4.186	3581s (00:59:41)
rmkk.by	IN	MX	preference: 10 exchange: mg1.g-cloud.by	3581s (00:59:41)
rmkk.by	IN	MX	preference: 20 exchange: ms1.g-cloud.by	3581s (00:59:41)
rmkk.by	IN	NS	a1.domain.by	3581s (00:59:41)
rmkk.by	IN	NS	a2.domain.by	3581s (00:59:41)
rmkk.by	IN	TXT	v=spf1 ip4:93.125.22.37 ip4:93.125.22.99 a mx ~all	3581s (00:59:41)
rmkk.by	IN	TXT	_globalsign-domain-verification=naRLTKCpsMpQUKPeU9-DDb8D_bH0-F9tUnGruxdqlX	3581s (00:59:41)
rmkk.by	IN	SOA	server: a1.domain.by email: info@domain.by serial: 2022060401 refresh: 43200 retry: 7200 expire: 2419200 minimum ttl: 11200	3581s (00:59:41)

Почтовый сервер организации – mg1.g-cloud.by.

Шаг 3. Выполним предыдущие проверки используя средства nslookup, host,dig.

```
┌──(alex㉿kali)-[~]
└─$ nslookup rmkk.by
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   rmkk.by
Address: 195.50.4.186
```

```
┌──(alex㉿kali)-[~]
└─$ host rmkk.by
rmkk.by has address 195.50.4.186
rmkk.by mail is handled by 20 ms1.g-cloud.by.
rmkk.by mail is handled by 10 mg1.g-cloud.by.

┌──(alex㉿kali)-[~]
└─$ dig rmkk.by

; <<>> DiG 9.18.4-2-Debian <<>> rmkk.by
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 348
9
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;rmkk.by.                       IN      A

;; ANSWER SECTION:
rmkk.by.                3523    IN      A       195.50.
4.186

;; Query time: 4 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Tue Dec 06 20:30:44 MSK 2022
;; MSG SIZE  rcvd: 41
```

Шаг 4. Определить DNS-имена и роли узлов из выделенных диапазонов IP-адресов. Использовать веб-средства http://dnsstuff.com и http://dnsreport.com.

SOA

TTL:
55 minutes 34 seconds

DATA: g-cloud.by. support.g-cloud.by. 2020041060 3600 3600 604800 86400

- **MNAME:** g-cloud.by.
- **RNAME:** support.g-cloud.by.
- **Serial:** 2020041060
- **Refresh:** 1 hour
- **Retry:** 1 hour
- **Expire:** 7 days
- **TTL:** 1 day

A

TTL:
55 minutes 34 seconds

DATA:
93.125.24.31

NS

TTL:
55 minutes 34 seconds

TARGET:
ns1.g-cloud.by.

TTL:
55 minutes 34 seconds

TARGET:
ns3.g-cloud.by.

TTL:
55 minutes 34 seconds

TARGET:
ns2.g-cloud.by.

MX

TTL:
55 minutes 34 seconds

EXCHANGE:
aspmx.l.google.com.uoggmk.by.

PREFERENCE:
3

TTL:
55 minutes 34 seconds

EXCHANGE:
alt2.aspmx.l.google.com.

PREFERENCE:
5

TTL:
55 minutes 34 seconds

EXCHANGE:
alt1.aspmx.l.google.com.

PREFERENCE:
5

TXT

TTL:
55 minutes 34 seconds

VALUE:
"v=spf1 include:_spf.g-cloud.by +mx -all"

Шаг 5. Проверим наличие узлов найденных сетей в базах данных спам-отправителей:

spamcop.net

Report Spam | Blocking List | Statistics | Login

Host rmkk.by (checking ip) = 195.50.4.186

Query bl.spamcop.net - 195.50.4.186

Lookup another:

(Help) (Trace IP) (TalosIntelligence Lookup)

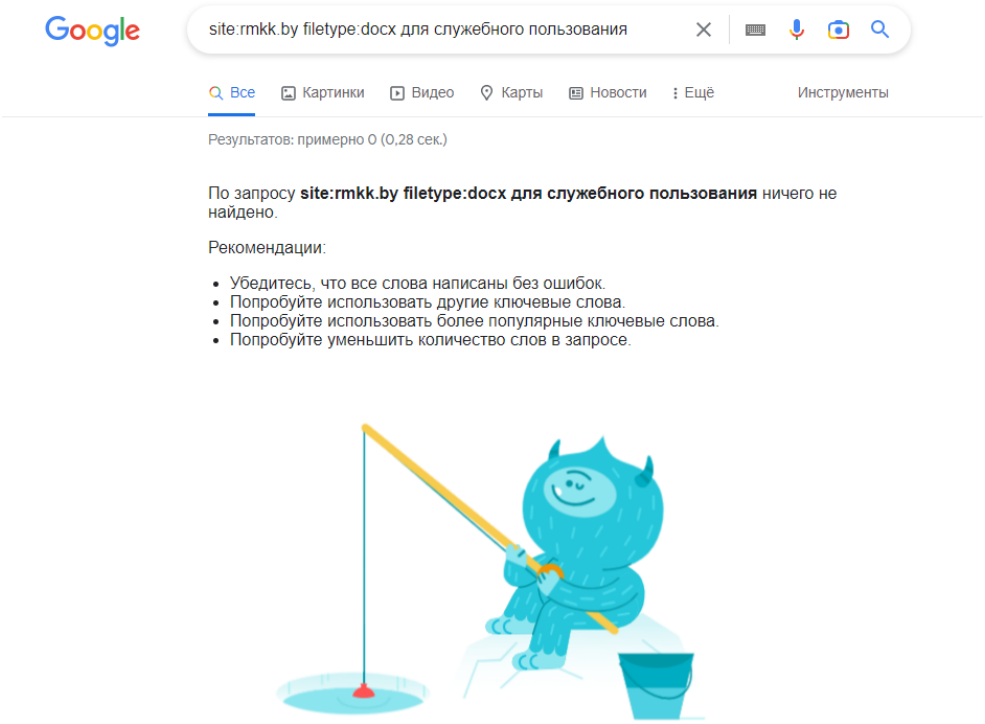
195.50.4.186 not listed in bl.spamcop.net

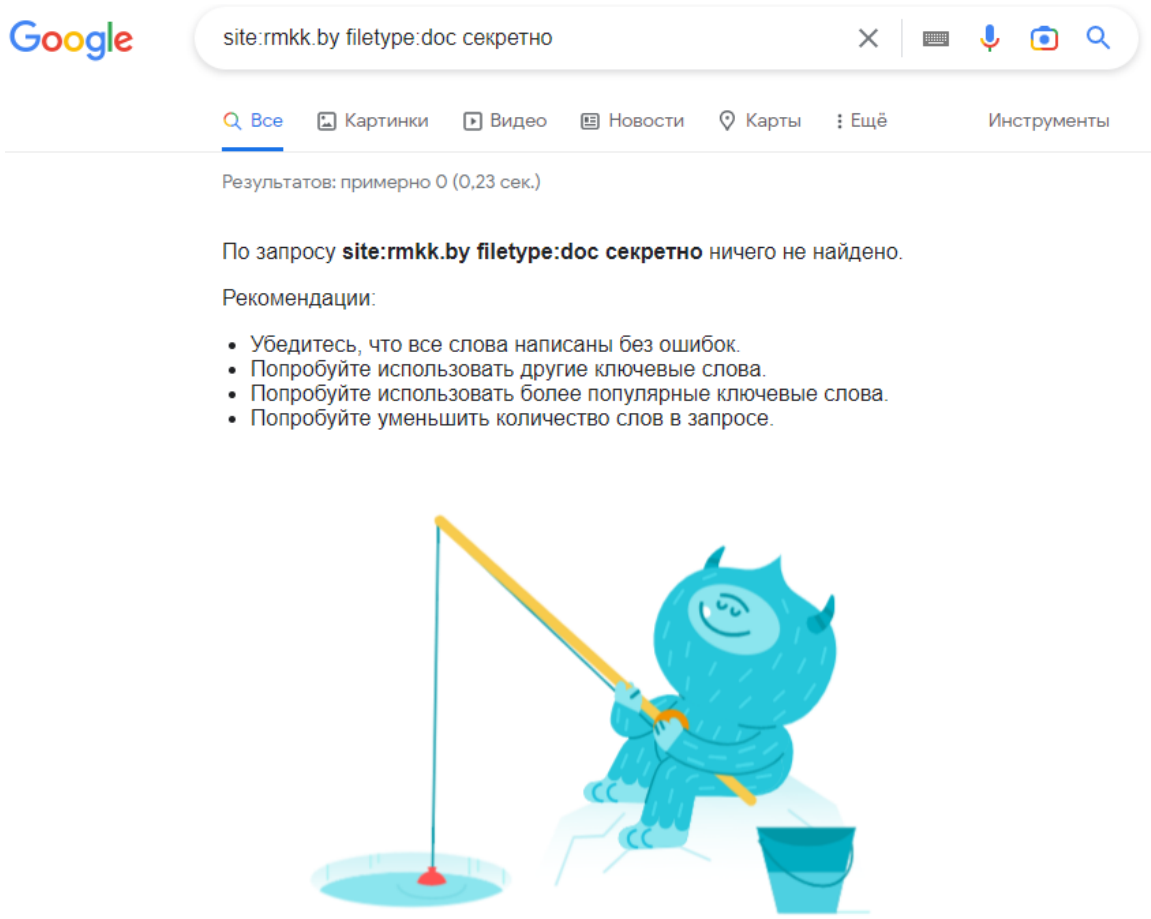
Шаг 6. Проверим возможность выполнения переноса зоны на первичном ивторичном DNS-серверах:

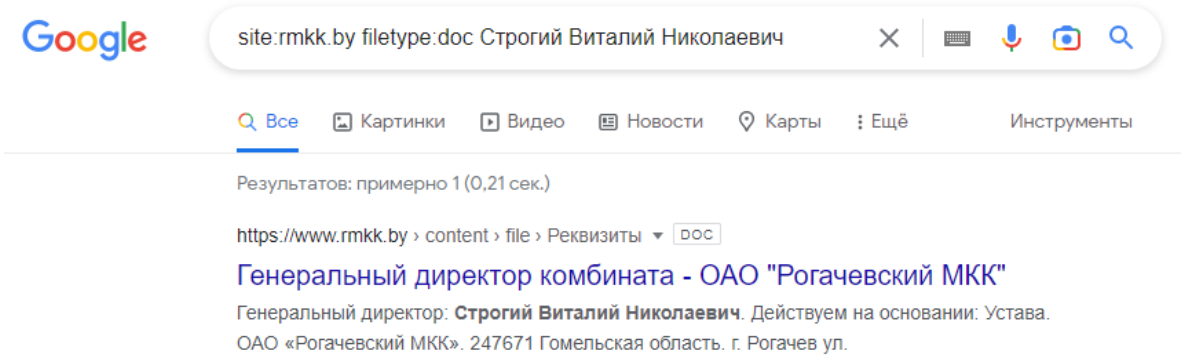
```
C:\Users\Alex>nslookup
╤хЁтхЁ яю єьюыўрэш■:  UnKnown
Address:  192.168.0.1

> server a1.domain.by
╤хЁтхЁ яю єьюыўрэш■:  a1.domain.by
Address:  193.232.92.25

> set type=any
> ls -d rmkk.by
[a1.domain.by]
*** Can't list domain rmkk.by: BAD ERROR VALUE
DNS-сервер отклонил передачу зоны rmkk.by на данный компьютер. Если это
ошибка, проверьте параметры безопасности передачи зоны для rmkk.by на DNS-
сервере по IP-адресу 193.232.92.25.
```

```
C:\Users\Alex>nslookup
╤хЁтхЁ яю єьюыўрэш■:  UnKnown
Address:  192.168.0.1

> server a2.domain.by
╤хЁтхЁ яю єьюыўрэш■:  a2.domain.by
Addresses:  2a02:2208:1:5::300
          93.84.119.236

> set type=any
> ls -d rmkk.by
ls: connect: No error
*** Can't list domain rmkk.by: Unspecified error
DNS-сервер отклонил передачу зоны rmkk.by на данный компьютер. Если это
ошибка, проверьте параметры безопасности передачи зоны для rmkk.by на DNS-
сервере по IP-адресу 2a02:2208:1:5::300.
```

Шаг 7. Найдём потенциально интересующую нас информацию в google.







Шаг 8. Используя веб-инструмент traceroute, расположенный на веб-ресурсе http://network-tools.com, определим маршруты прохождения IP-дейтаграмм доисследуемой сети.

Traceroute for rmkk.by with a maximum of 15 hops.

Destination: 195.50.4.186

Hop #1	216.182.239.39	7.896 ms
Hop #2	100.65.51.64	4.599 ms
Hop #3	100.66.29.140	20.761 ms
Hop #4	100.66.30.156	5.384 ms
Hop #5	100.66.3.63	2.435 ms
Hop #6	100.66.0.79	9.828 ms
Hop #7	100.65.97.132	5.247 ms
Hop #8	100.66.48.18	7.230 ms
Hop #9	100.66.51.254	13.255 ms
Hop #10	241.0.4.196	0.217 ms
Hop #11	240.0.36.19	0.340 ms
Hop #12	240.0.36.30	0.235 ms
Hop #13	242.0.170.129	0.267 ms
Hop #14	52.93.28.139	1.207 ms
Hop #15	100.100.8.70	1.026 ms

Вывод: в ходе лабораторной работы изучили методы и средства сбора предварительной информации в Интернет об анализируемой компьютерной сети.