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
Созинов Л.В.
Проверил:
Грищенко В.В.

2022

Лабораторная работа №1
Сбор предварительной информации

Цель работы: Обучение методам и средствам сбора предварительной информации в Интернет об анализируемой КС.

Постановка задачи: выполнить предварительный сбор информации о домене spartak.by. Работа выполняется на АРМ, имеющем доступ в сеть Интернет.

Ход работы

1. Перейти по адресу https://www.whois.com Проанализировать полученные данные. Найти DNS-имена и IP-адреса серверов имен.

Результаты проверки домена spartak.by

Информация о домене

Регистратор:

ООО "Белорусские облачные технологии"
Belarusian Cloud Technologies LLC

Владелец домена:

СП ОАО Спартак
BY, г. Гомель, -, 246000, ул. Советская, 63, -
Регистрационный или иной идентификационный номер: 400078278
Телефон: +375 232 304477
E-mail: admin@spartak.by

DNS-серверы:

ns1.g-cloud.by
ns2.g-cloud.by
ns3.g-cloud.by

Состояние:

Дата создания: 2002-11-21
Дата последнего обновления: 2022-04-27
Дата окончания: 2023-12-26

spartak.by

Updated 1 second ago

```
Domain name: spartak.by
Registrar: Belarusian Cloud Technologies LLC
Org: СП ОАО Спартак
Country: BY
Address: 246000, -, г. Гомель, ул. Советская, 63, -
Registration or other identification number: 400078278
Phone: +375 232 304477
Email: HIDDEN! Details are available at https://whois.cctld.by
Name Server: ns1.g-cloud.by
Name Server: ns2.g-cloud.by
Name Server: ns3.g-cloud.by
Update Date: 2022-04-27
Creation Date: 2002-11-21
Expiration Date: 2023-12-25

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

2. Перейти по адресу http://network-tools.com/nslook. Определить почтовый сервер организации.

Answer records

name	class	type	data	time to live
spartak.by	IN	SOA	server: g-cloud.by email: tech@g-cloud.by serial: 2022042635 refresh: 10800 retry: 3600 expire: 604800 minimum ttl: 86400	3600s (01:00:00)
spartak.by	IN	A	93.125.24.40	3600s (01:00:00)
spartak.by	IN	NS	ns2.g-cloud.by	3600s (01:00:00)
spartak.by	IN	NS	ns1.g-cloud.by	3600s (01:00:00)
spartak.by	IN	NS	ns3.g-cloud.by	3600s (01:00:00)
spartak.by	IN	MX	preference: 10 exchange: mg1.g-cloud.by	3600s (01:00:00)
spartak.by	IN	MX	preference: 20 exchange: ms8.g-cloud.by	3600s (01:00:00)
spartak.by	IN	TXT	MS=BB8320794D8DA4D0F1AA6BE85527102CF14CB895	3600s (01:00:00)
spartak.by	IN	TXT	v=spf1 include:_spf.g-cloud.by +mx -all	3600s (01:00:00)

Почтовые сервера организации находятся под типом Mx.

3. Выполнить предыдущие проверки, используя средства host и dig.

```
└─$ host spartak.by
spartak.by has address 93.125.24.40
spartak.by mail is handled by 20 ms8.g-cloud.by.
spartak.by mail is handled by 10 mg1.g-cloud.by.
```

```
└─$ dig spartak.by

; <<>> DiG 9.18.4-2-Debian <<>> spartak.by
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34998
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
spartak.by.             1251    IN      A       93.125.24.40

;; Query time: 4 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Tue Dec 06 20:42:29 MSK 2022
;; MSG SIZE  rcvd: 44
```

```
└─$ nslookup spartak.by
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   spartak.by
Address: 93.125.24.40
```

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

TXT

TTL:

1 hour

VALUE:

"MS=BB8320794D8DA4D0F1AA6BE85527102CF14CB895"

TTL:

1 hour

VALUE:

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

MX

TTL:

1 hour

EXCHANGE:

ms8.g-cloud.by.

PREFERENCE:

20

TTL:

1 hour

EXCHANGE:

mg1.g-cloud.by.

PREFERENCE:

10

SOA

TTL:

1 hour

DATA: g-cloud.by. tech.g-cloud.by. 2022042635 10800 3600 604800 86400

- MNAME: g-cloud.by.
- RNAME: tech.g-cloud.by.
- Serial: 2022042635
- Refresh: 3 hours
- Retry: 1 hour
- Expire: 7 days
- TTL: 1 day

NS

TTL:

1 hour

TARGET:

ns1.g-cloud.by.

TTL:

1 hour

TARGET:

ns3.g-cloud.by.

TTL:

1 hour

TARGET:

ns2.g-cloud.by.

A

TTL:

1 hour

DATA:

93.125.24.40

5. Проверить наличие узлов найденных сетей в базах данных спам-отправителей и бот-сетях.

Host spartak.by (checking ip) = 93.125.24.40

Query bl.spamcop.net - 93.125.24.40

Lookup another:

(Help) (Trace IP) (TalosIntelligence Lookup)

93.125.24.40 not listed in bl.spamcop.net

6. Проверить возможность выполнения переноса зоны на первичном и вторичном DNS-серверах.

```
C:\Users\Lndidro>nslookup
╤хЁтхЁ яю ебюыўрэш■:  UnKnown
Address:  192.168.0.1

> server ns1.g-cloud.by
╤хЁтхЁ яю ебюыўрэш■:  ns1.g-cloud.by
Address:  195.50.4.201

> set type=any
> ls -d spartak.by
[ns1.g-cloud.by]
*** Can't list domain spartak.by: Query refused
DNS-сервер отклонил передачу зоны spartak.by на данный компьютер. Если это
ошибка, проверьте параметры безопасности передачи зоны для spartak.by на DNS-
сервере по IP-адресу 195.50.4.201.
```

```
C:\Users\Lndidro>nslookup
╤хЁтхЁ яю ебюыўрэш■:  UnKnown
Address:  192.168.0.1

> server ns2.g-cloud.by
╤хЁтхЁ яю ебюыўрэш■:  ns2.g-cloud.by
Addresses:  2a00:c827:6:3:1c00:4dff:fe00:93
          195.50.11.20

> set type=any
> ls -d spartak.by
ls: connect: Result too large
*** Can't list domain spartak.by: Unspecified error
DNS-сервер отклонил передачу зоны spartak.by на данный компьютер. Если это
ошибка, проверьте параметры безопасности передачи зоны для spartak.by на DNS-
сервере по IP-адресу 2a00:c827:6:3:1c00:4dff:fe00:93.
```

7. Перейти по адресу http://google.ru. Задать следующие поисковые запросы и проанализировать результаты.

site:spartak.by filetype:doc Горбачев

Все | Картинки | Новости | Видео | Карты | Ещё | Инструменты

Результатов: примерно 0 (0,24 сек.)

По запросу **site:spartak.by filetype:doc Горбачев** ничего не найдено.

Рекомендации:

- Убедитесь, что все слова написаны без ошибок.
- Попробуйте использовать другие ключевые слова.
- Попробуйте использовать более популярные ключевые слова.
- Попробуйте уменьшить количество слов в запросе.

site:spartak.by filetype:docx секретно

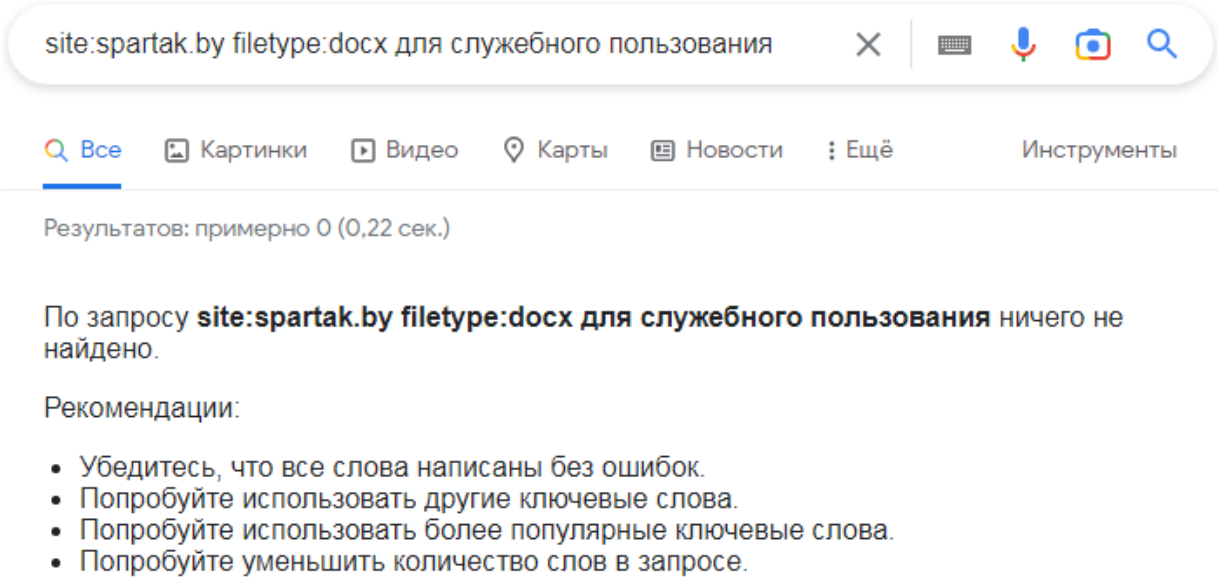
Все | Картинки | Видео | Новости | Карты | Ещё | Инструменты

Результатов: примерно 0 (0,24 сек.)

По запросу **site:spartak.by filetype:docx секретно** ничего не найдено.

Рекомендации:

- Убедитесь, что все слова написаны без ошибок.
- Попробуйте использовать другие ключевые слова.
- Попробуйте использовать более популярные ключевые слова.
- Попробуйте уменьшить количество слов в запросе.



8. Используя веб-инструмент traceroute, расположенный на вебресурсе http://network-tools.com, определить маршруты прохождения IP-дейтаграмм до исследуемой сети.

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

Destination: 93.125.24.40

Hop #1	3.236.60.39	4.590 ms
Hop #2	100.65.60.64	6.367 ms
Hop #3	100.66.24.88	4.591 ms
Hop #4	100.66.26.238	17.056 ms
Hop #5	100.66.2.237	8.366 ms
Hop #6	100.66.4.229	1.320 ms
Hop #7	100.65.106.130	6.207 ms
Hop #8	100.66.48.150	43.896 ms
Hop #9	100.66.51.190	11.335 ms
Hop #10	241.0.4.95	0.240 ms
Hop #11	240.0.40.31	0.218 ms
Hop #12	240.0.36.28	0.239 ms
Hop #13	242.0.162.161	0.285 ms
Hop #14	52.93.28.167	0.863 ms
Hop #15	100.100.6.80	1.026 ms