

Гомельский Государственный Университет
им. Ф. Скорины

Лабораторная работа №1.
Сбор предварительной информации

Проверил:

Грищенко В.В.

Студент МС – 42:

Черненко А.В.

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

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

Последовательность действий

Шаг 1. Перейти по адресу <https://whois.by>. Указать в строке поиска в базе данных доменов vsmu.by. Проанализировать полученные данные. Найти DNS-имена. Проанализировать данные по администраторам и контактным лицам организации. Найти используемые почтовые адреса.

Результаты проверки домена:
vsmu.by

Информация о домене

Регистратор:

Открытый контакт
Open Contact, Ltd

Владелец домена:

УО "Витебский государственный ордена Дружбы народов медицинский университет"
Страна: Беларусь (BY)
Адрес: 210009, Витебская, Витебск, пр-т Фрунзе, д.27, 215
Регистрационный или иной идентификационный номер: 300002704
Телефон: +375212261093
Email: vgmuby@gmail.com

DNS-серверы:

a1.domain.by
a2.domain.by

Состояние *:

Дата создания: 16-11-2012
Дата последнего обновления: 24-09-2020
Дата окончания: 16-11-2022

* время указано по часовому поясу UTC+03:00

Шаг 2. Перейти по адресу <http://network-tools.com/nslookup>. Задать параметры: домен – vsmu.by, тип запроса – ANY. Определить почтовый сервер организации.

DNS Records for: 'vsmu.by'

Returned Data

Name	TTL Until Refresh	Class	Type	Data
vsmu.by.	10800	IN	A	134.17.89.86
vsmu.by.	10800	IN	NS	a1.domain.by.
vsmu.by.	10800	IN	NS	a2.domain.by.
vsmu.by.	10800	IN	SOA	a1.domain.by. info\@domain.by. 1596705249 10800 3600 604800 300
vsmu.by.	10800	IN	MX	10 mail.vsmu.by.

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

```
alexandr@alexandr-N550JK: ~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
alexandr@alexandr-N550JK:~$ nslookup vsmu.by  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
Name:   vsmu.by  
Address: 134.17.89.86  
  
alexandr@alexandr-N550JK:~$ host vsmu.by  
vsmu.by has address 134.17.89.86  
vsmu.by mail is handled by 10 mail.vsmu.by.  
alexandr@alexandr-N550JK:~$ dig vsmu.by  
  
; <>> DiG 9.11.3-lubuntu1.11-Ubuntu <>> vsmu.by  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13145  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags;; udp: 65494  
;; QUESTION SECTION:  
vsmu.by.                IN      A  
  
;; ANSWER SECTION:  
vsmu.by.                1405    IN      A      134.17.89.86  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53)  
;; WHEN: Tue Dec 22 19:47:19 +03 2020  
;; MSG SIZE rcvd: 52  
  
alexandr@alexandr-N550JK:~$
```

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

DNSreport Results for vsmu.by

Export

Overall Results:

1

FAIL

3

WARNING

21

PASS

4

INFO

PARENT

Status	Test Name	Information
WARN	Parent zone provides NS records	<p>Parent zone does not provide glue for nameservers, which will cause delays in resolving your domain name. The following nameserver addresses were not provided by the parent 'glue' and had to be looked up individually. This is perfectly acceptable behavior per the RFCs. This will usually occur if your DNS servers are not in the same TLD as your domain (for example, a DNS server of "ns1.example.org" for the domain "example.com"). In this case, you can speed up the connections slightly by having NS records that are in the same TLD as your domain.</p> <p>a2.domain.by. No Glue TTL=3600 a1.domain.by. No Glue TTL=3600</p>
PASS	Number of nameservers	<p>At least 2 (RFC2182 section 5 recommends at least 3), but fewer than 8 NS records exist (RFC1912 section 2.8 recommends that you have no more than 7). This meets the RFC minimum requirements, but is lower than the upper limits that some domain registrars have on the number of nameservers. A larger number of nameservers reduce the load on each and, since they should be located in different locations, prevent a single point of failure. The NS Records provided are:</p> <p>a2.domain.by. No Glue TTL=3600 a1.domain.by. No Glue TTL=3600</p>

NS

Status	Test Name	Information
PASS	Unique nameserver IPs	<p>All nameserver addresses are unique. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data:</p> <p>a1.domain.by. No Glue a2.domain.by. No Glue</p>
PASS	All nameservers respond	<p>All nameservers responded. We were able to get a timely response for NS records from your nameservers, which indicates that they are running correctly and your zone (domain) is valid. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data:</p> <p>a1.domain.by. No Glue a2.domain.by. No Glue</p>
PASS	Open DNS servers	<p>Nameservers do not respond to recursive queries. Your DNS servers do not announce that they are open DNS servers (i.e. answering recursively). Although there is a slight chance that they really are open DNS servers, this is very unlikely. Open DNS servers increase the chances of cache poisoning, can degrade performance of your DNS, and can cause your DNS servers to be used in an attack, so it is imperative that externally facing DNS servers do not recursively answer queries.</p>
PASS	All nameservers authoritative	<p>All nameservers answered authoritatively for the zone. This indicates that the zones for this domain are set up correctly on your nameservers and that we should be able to get good responses to further queries.</p>
PASS	NS list matches parent list	<p>NS list matches list from parent zone. This indicates that your parent nameservers are 'aware' of the correct authoritative nameservers for your domain. This ensures less overhead for DNS queries, because an extra DNS resolution step is not required.</p>
PASS	NS address list matches parent zone	<p>NS addresses matches list from parent zone. This indicates that your parent nameservers are 'aware' of the correct authoritative nameservers for your domain. This ensures less overhead for DNS queries, because an extra DNS resolution step is not required.</p>
PASS	Stealth nameservers	<p>No stealth nameservers discovered. There is very little chance that there will be 'confusion' when resolving your domain records from the parent nameservers. There appear to be no 'extra' nameservers listed that the parent might try to refer to and cause DNS resolution delays.</p>
INFO	Stealth nameservers respond	<p>No stealth nameservers to test. This is simply a note to indicate that you do not have any stealth nameservers to test, which is what is normally expected of domains.</p>
PASS	TCP allowed	<p>All nameservers respond to queries via TCP. It is important that your DNS servers respond to both TCP and UDP connections. TCP Port 53 is used for large queries and responses, zone transfers, and is part of the DNSSEC standard.</p>
PASS	Nameserver software version	<p>Responses from nameservers do not appear to be version numbers. While version information is important internally, DNS version information displayed externally can leave your servers vulnerable to version-specific exploits. Your servers appear to hide this information and are likely safer.</p>
PASS	All nameservers have identical records	<p>All of your nameservers are providing the same list of nameservers.</p>
PASS	All nameserver addresses are public	<p>All of your nameserver addresses are public. If there were any private IPs, they would not be reachable, causing DNS delays.</p>

Шаг 5. Проверить наличие узлов найденных сетей в базах данных спам-отправителей и бот-сетях, используя для этого веб-средства <http://www.spamcop.net> и <http://rbls.org>.

vsmu.by

updated:

DNSBL stands for DNS block list, previously more commonly called RBL as in Realtime Block List

contacts.abuse.net

ex.dnsbl.org

in.dnsbl.org

whois.rfc-clueless.org

0spamurl.fusionzero.com

_vouch.dwl.spamhaus.org

abuse.rfc-clueless.org

abuse.rfc-ignorant.org

bl.deadbeef.com

blacklist.netcore.co.in

bogusmx.rfc-clueless.org

bogusmx.rfc-ignorant.org

bsb.empty.us

bsb.spamlookup.net

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

C:\nslookup

>server ns.vsmu.by

>set type=any

>vsmu.by

```
C:\Users\Александр>nslookup
DNS request timed out.
    timeout was 2 seconds.
ТхЁтхЁ яю ёьюйрэш■: UnKnown
Address: 192.168.43.1

> ns1.vsmu.by
ТхЁтхЁ: UnKnown
Address: 192.168.43.1

Ль : ns1.vsmu.by
Addresses: 52.214.129.184
          52.209.63.28

> set type=any
> vsmu.by
ТхЁтхЁ: UnKnown
Address: 192.168.43.1

Не заслуживающий доверия ответ:
vsmu.by internet address = 134.17.89.86
vsmu.by nameserver = a2.domain.by
vsmu.by nameserver = a1.domain.by
```

Шаг 7. Перейти по адресу <http://google.ru>. Задать следующие поисковые запросы и проанализировать результаты:
«site:vsmu.by filetype:docx для служебного пользования»;

Google search results for the query "site:vsmu.by filetype:docx для служебного пользования". The search bar shows the query and the Google logo. Below the search bar, there are navigation links: "Усе", "Відарысы", "Болей", "Налады", and "Інструменты". The results show 5 items (0,30 c).

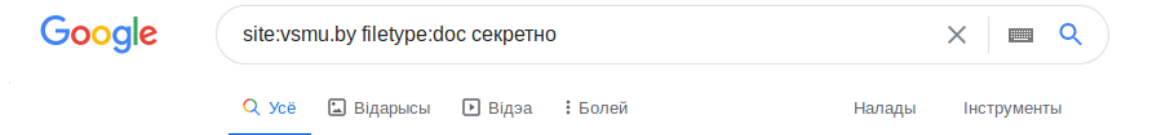
- do2.vsmu.by > mod > view > DOC Перакладзі гэту старонку
ТЕРМИНОЛОГИЧЕСКИЙ СЛОВАРЬ
... связанные с осуществлением ими правомочий владения, пользования и распоряжения ... **Служебный** объект промышленной собственности - объект ...
- www.vsmu.by > vospet > Ин... > DOC Перакладзі гэту старонку
Статья 55. Клятва врача Республики Беларусь - Витебский ...
Пользование предусмотренными в пункте 2 настоящей статьи правами ... **служебное** удостоверение журналиста средства массовой информации, ...
- do2.vsmu.by > mod > view > DOC Перакладзі гэту старонку
10. Смета организаций здравоохранения
... и предметов длительного пользования (подстатья 2400100); капитальный ... **служебные** разъезды" предусматриваются расходы (затраты) на оплату:..
- do2.vsmu.by > pluginfile.php > mod_folder > content > DOC
4.8. Функциональные обязанности главной медицинской ...
... высовываться и переговариваться через окно;; пользоваться **служебным** ... центров коллективного **пользования** оборудования» в организациях ...
- do2.vsmu.by > mod > view > DOC > Перакладзі гэту старонку
ПОСТАНОВЛЕНИЕ ПРАВЛЕНИЯ НАЦИОНАЛЬНОГО ...
В этом случае расходы по проезду к месту **служебной** командировки и ... процентов и плату за **пользование** кредитом, уплату неустойки (штрафа, пени) ...

«site:vsmu.by filetype:pdf для служебного пользования»;

Google search results for the query "site:vsmu.by filetype:pdf для служебного пользования". The search bar shows the query and the Google logo. Below the search bar, there are navigation links: "Все", "Картинки", "Видео", "Карты", "Новости", "Ещё", "Настройки", and "Инструменты". The results show approximately 132 items (0,38 сек.).

- elib.vsmu.by > bitstream > med_2004_690-693
Медицинское образование XXI века - Электронный архив ...
для **служебного пользования**, консультации преподавателей кафедры. В настоящее время разрабатываются предложения (при подготовке офицеров ...
- profsotr.vsmu.by > 01_all_site > Kollektivnij_dogovor > PDF
лдално - Профком сотрудников ВГМУ
Настоящее положение о **служебных** командировках работников ... 4.3.1. по проезду транспортом общего **пользования** (кроме такси) к станции, пристани ...
- profsotr.vsmu.by > 01_all_site > 2017_02_izmenenija > PDF
Приложение № 7 к коллективному договору Учреждение ...
1.1 Настоящее Положение о **служебных** командировках работников ... 4.3.1. по проезду транспортом общего **пользования** (кроме такси) к станции ...
- www.vsmu.by > images > files > abit > Положение_об... > PDF
Положение об общежитии - ВГМУ
общежитии), владение и **пользование** им, заключения договора найма ... погибших (умерших) в мирное время при выполнении **служебных**.

«site:vsmu.by filetype:doc секретно»;

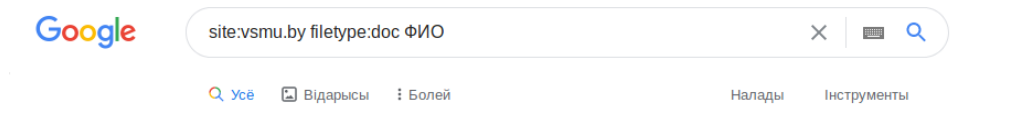


Па запыце **site:vsmu.by filetype:doc секретно** нічога не знойдзена

Прапановы:

- Праверце правапіс усіх слоў
- Паспрабуйце іншыя ключавыя словы.
- Паспрабуйце больш агульныя ключавыя словы.
- Паспрабуйце ўжыць менш ключавых слоў

«site:vsmu.by filetype:doc ФИО»



Вынікаў каля 182 (0,33 с)

www.vsmu.by > practic > lech > [DOC] [Перакладзі гэту старонку](#)

Уважаемые студенты 3-5 курсов

ФИО, Группа. 1, Реут Кирилл Валентинович, 2, 2, Петров Иван Сергеевич, 10, 3, Рубцов Илья Юрьевич, 10, 4, Боровикова Мария Алексеевна, 26.

www.vsmu.by > practic > lech > [DOC] [Перакладзі гэту старонку](#)

Уважаемые студенты 3-5 курсов - ВГМУ

ФИО, Группа. 1, Реут Кирилл Валентинович, 2, 2, Петров Иван Сергеевич, 10, 3, Рубцов Илья Юрьевич, 10, 4, Боровикова Мария Алексеевна, 26.

www.vsmu.by > images > П... > [DOC] [Перакладзі гэту старонку](#)

Студенческий олимп

№п/п, ФИО, Курс, Группа, Ср. балл. Апёнок Ольга Александровна, 2, 10, 9,00. Белогородская Полина Викторовна, 2, 30, 9,00. Гапова Елизавета ...

www.vsmu.by > practic > lech > [DOC] [Перакладзі гэту старонку](#)

О производственной врачебной

ФИО студента, № гр. Сроки практики. УЗ «Витебская ГКП №1». Терапевтическое отд. Хирургическое отд. Группа №1, 03.08-14.08, 17.08-28.08. 1, Кажуро ...

www.vsmu.by > practic > lech > [DOC] [Перакладзі гэту старонку](#)

О производственной амбулаторно-поликлинической

ФИО студента, № гр. Сроки практики. Центральная городская п-ка. (ул. Терешковой). Терапевтическое отд. Хирургическое отд. Группа №1, 29.06 – 10.07 ...

www.vsmu.by > practic > lech > [DOC] [Перакладзі гэту старонку](#)


Вниманию студентов ВГМУ 5 курса лечебного факультета ...

Фамилия, имя, отчество. Дата рождения _____
Пол: мужской / женский ... ФИО пациента (полностью) ...

www.vsmu.by > files > practic > [DOC] [Перакладзі гэту старонку](#)

Шаг 8. Используя веб-инструмент traceroute, расположенный на вебресурсе <http://network-tools.com>, определить маршруты прохождения IPдейтаграмм до исследуемой сети.

Online service Traceroute

 **Traceroute** - Traces the route of packets to destination host from our server

IP address or host name:

134.17.89.86

Enter code:

TRST

Go

traceroute to 134.17.89.86 (134.17.89.86), 30 hops max, 60 byte packets

1				*	*	*
2	core23.fsn1.hetzner.com	213.239.245.237	de	5.023 ms	*	5.006 ms
3	core0.fra.hetzner.com	213.239.252.41	de	19.790 ms		
	core4.fra.hetzner.com	213.239.229.73	de	6.613 ms		
	core0.fra.hetzner.com	213.239.252.41	de	19.790 ms		
4	mac-18-de-d7-eb-be-a8.ipv4-080-081-195-197.pas-25465.20giga.de-cix.fra.de.as60280.ntec.by	80.81.195.197	de	29.965 ms	30.187 ms	30.326 ms