Лабораторна робота № 5(3.1.9)
DNS запити
Хід роботи:

Частина 1: Використання nslookup для отримання інформації про домени та IP адреси

Крок 1: Вхід в Kali Linux та доступ до терміналу

Команди:

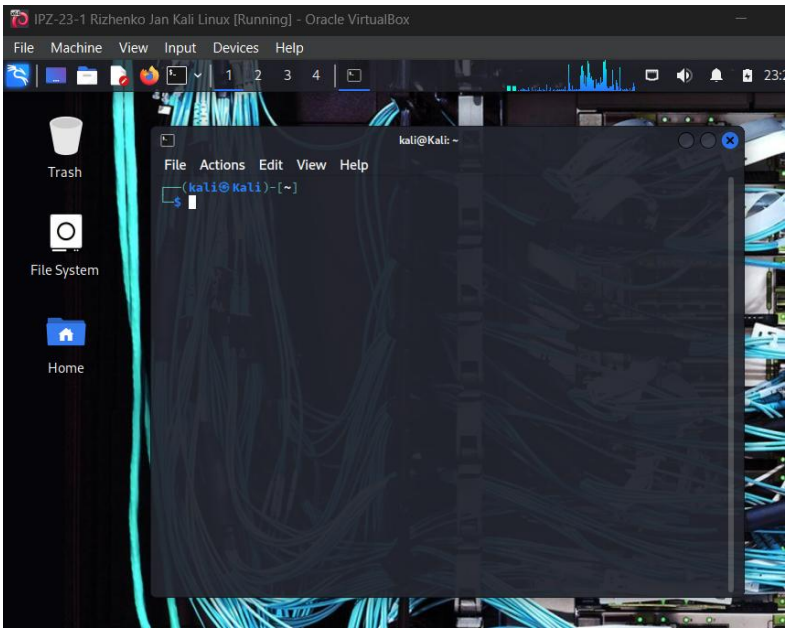

Рис. 1. Термінал відкрито.

Крок 2: Дослідження можливостей nslookup

Команда для перегляду manual pages:

```
┌──(kali㉿Kali)-[~]
└─$ man nslookup
```

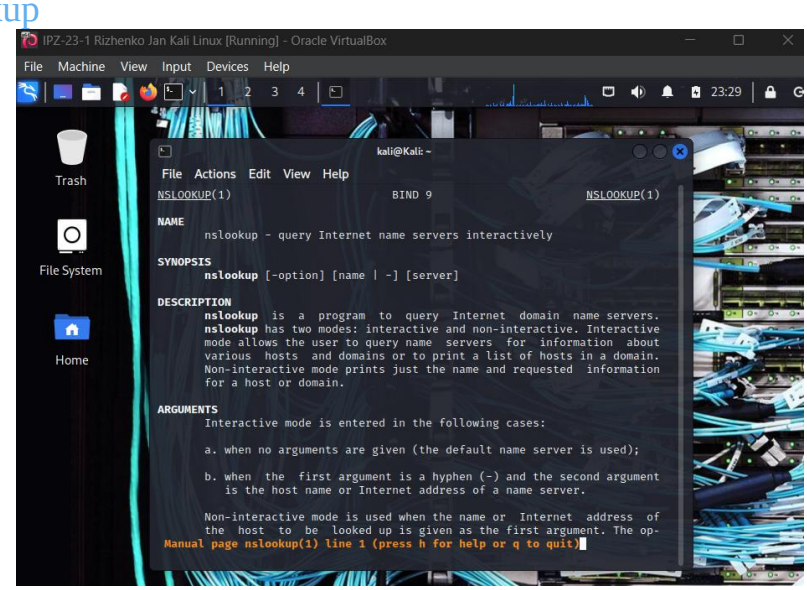

Рис. 2. Man nslookup

Для перегляду сторінок використовується пробіл. Для виходу q.

Питання: Яке ключове слово set ви б використали для запиту MX запису поштового сервера в домені?

Відповідь:

set type=mx

або

set querytype=mx

Крок 3: Використання команди nslookup

Команди для інтерактивного режиму:

```
┌──(kali㉿Kali)-[~]
└─$ nslookup
# Запит домену cisco.com
# Змінити тип запиту на NS (name servers)
# Запит домену cisco.com
# Вийти з інтерактивного режиму
```

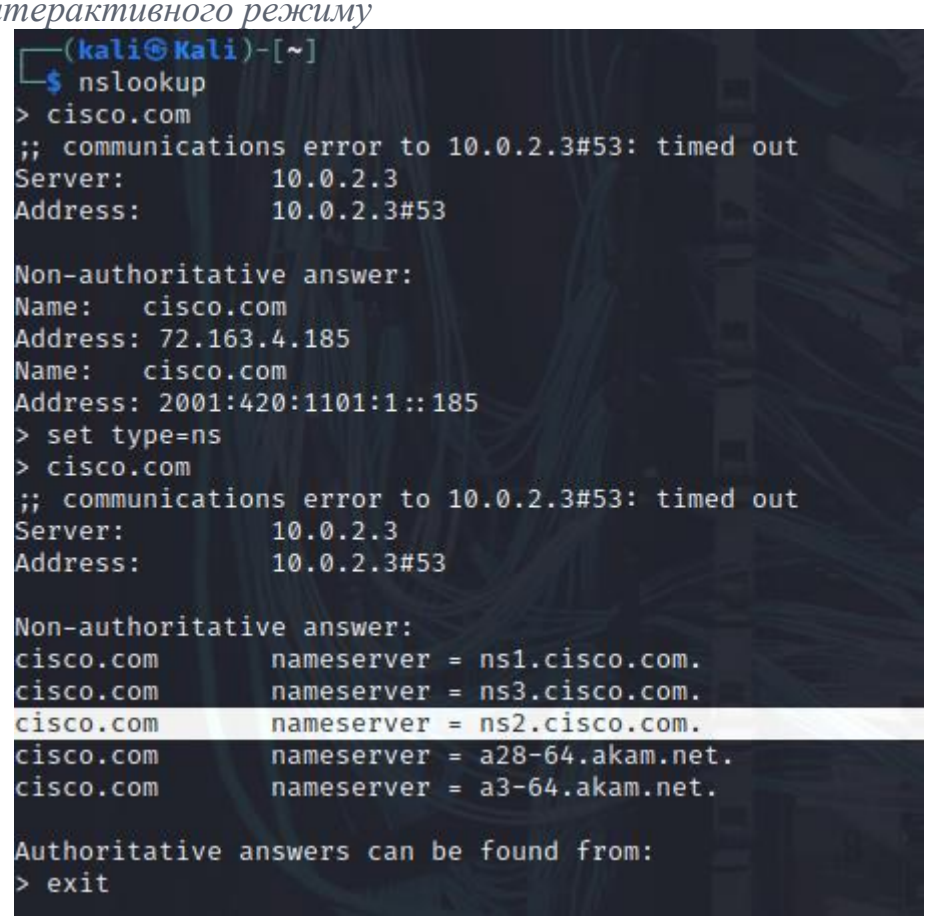

Рис. 3. Виконані дії у nslookup.

Питання: Які IPv4 та IPv6 адреси первинного DNS сервера (ns1)?

Відповідь:

IPv4: 72.163.4.185

IPv6: 2001:420:1101:1::185

Крок 4: Зміна сервера для виконання запитів

Команди для використання іншого DNS сервера:

```
# Однорядковий синтаксис (неінтерактивний режим)
# Інтерактивний режим
```

```
┌──(kali㉿Kali)-[~]
└─$ nslookup skillsforall.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   skillsforall.com
Address: 108.138.51.66
Name:   skillsforall.com
Address: 108.138.51.45
Name:   skillsforall.com
Address: 108.138.51.97
Name:   skillsforall.com
Address: 108.138.51.73


┌──(kali㉿Kali)-[~]
└─$ nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> skillsforall.com
;; communications error to 8.8.8.8#53: timed out
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   skillsforall.com
Address: 108.138.51.66
Name:   skillsforall.com
Address: 108.138.51.97
Name:   skillsforall.com
Address: 108.138.51.45
Name:   skillsforall.com
Address: 108.138.51.73
> 
```

Рис. 4. Виконані дії у nslookup.

Команди для запиту всіх типів записів (ANY):

```
> set type=any
> skillsforall.com
;; Connection to 8.8.8.8#53(8.8.8.8) for skillsforall.com failed: timed out.
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   skillsforall.com
Address: 108.138.51.97
Name:   skillsforall.com
Address: 108.138.51.45
Name:   skillsforall.com
Address: 108.138.51.66
Name:   skillsforall.com
Address: 108.138.51.73
skillsforall.com        nameserver = ns-588.awsdns-09.net.
skillsforall.com        nameserver = ns-1652.awsdns-14.co.uk.
skillsforall.com        nameserver = ns-1130.awsdns-13.org.
skillsforall.com        nameserver = ns-489.awsdns-61.com.
skillsforall.com
        origin = ns-1130.awsdns-13.org
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400
skillsforall.com        mail exchanger = 10 inbound-smtp.us-east-1.amazonaws.
com.
skillsforall.com        text = "facebook-domain-verification=8cg08gu4eikp0d2d
1quqhjwh5ti1vv"
skillsforall.com        text = "google-site-verification=Q5NIWRygJYTSLxuHReNK
w1kvgC8IXKTOyPf5zITDv40"
skillsforall.com        text = "d1g1l9y74sxj8m.cloudfront.net"
skillsforall.com        text = "identrust_validate=XzTu3rqoVVwnwNykPpaGYBeA4d
e5HaSynIEnsHWXyIur"
skillsforall.com        text = "v=spf1 include:amazonses.com ~all"

Authoritative answers can be found from:
> 
```

Рис. 5. Виконані дії з type=any.

Питання: Які типи записів відображаються у виводі команди nslookup з типом set to any?
Відповідь:
У виводі команди nslookup з типом "any" відображаються наступні типи записів:
A - IPv4 адреси (Address)
AAAA - IPv6 адреси
NS - Name Server записи (nameserver)
MX - Mail Exchanger записи (mail exchanger)
TXT - Text записи (text)
SOA - Start of Authority (origin, serial, refresh, retry, expire, minimum)
Частина 2: Використання команди whois для пошуку додаткової реєстраційної інформації
Крок 1: Порівняння виводу whois для різних організацій

```
┌──(kali㉿Kali)-[~]
└─$ whois cisco.com
   Domain Name: CISCO.COM
   Registry Domain ID: 4987030_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2025-04-13T10:06:28Z
   Creation Date: 1987-05-14T04:00:00Z
   Registry Expiry Date: 2026-05-15T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeletePr
ohibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransf
erProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdatePr
ohibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeletePr
ohibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransf
erProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdatePr
ohibited
   Name Server: A28-64.AKAM.NET
   Name Server: A3-64.AKAM.NET
   Name Server: NS1.CISCO.COM
   Name Server: NS2.CISCO.COM
   Name Server: NS3.CISCO.COM
```

Рис. 6. Запит інформації про cisco.com.

```
┌──(kali㉿Kali)-[~]
└─$ whois skillsforall.com
   Domain Name: SKILLSFORALL.COM
   Registry Domain ID: 1823854105_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2025-04-14T17:29:11Z
   Creation Date: 2013-08-27T18:04:50Z
   Registry Expiry Date: 2026-08-27T18:04:50Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeletePr
ohibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransf
erProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdatePr
ohibited
   Name Server: NS-1130.AWSDNS-13.ORG
   Name Server: NS-1652.AWSDNS-14.CO.UK
   Name Server: NS-489.AWSDNS-61.COM
   Name Server: NS-588.AWSDNS-09.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wi
cf/
```

Рис. 7. Запит інформації про skillsforall.com.

Питання: Який висновок ви можете зробити про два домени (cisco.com та skillsforall.com) на основі виводу команд whois?
На основі виводу команд whois можна зробити наступні висновки:
cisco.com:
Домен зареєстрований безпосередньо на Cisco Systems, Inc.

Реєстраційна інформація містить деталі про організацію (адреса: 170 West Tasman Drive, San Jose, CA)
Показує технічні та адміністративні контакти Cisco
Домен зареєстрований через MarkMonitor Inc. (корпоративний реєстратор)
Інформація є відкритою та детальною
skillsforall.com:
Домен, ймовірно, зареєстрований через хостинг-провайдера або використовує захист приватності
Може використовувати AWS (Amazon Web Services) для хостингу, як видно з NS записів
Реєстраційна інформація може бути захищена (privacy protection)
Менше прямої контактної інформації про організацію
Висновок: cisco.com є великою корпоративною організацією з прозорою реєстрацією, тоді як skillsforall.com може бути меншою організацією або використовувати послуги хмарного хостингу з приватною реєстрацією.
Крок 2: Використання whois для визначення інформації про реєстрацію IP адрес
 # Запит інформації про IP адресу DNS сервера Cisco

```
┌──(kali㉿Kali)-[~]
└─$ whois 72.163.5.201
```

 # Запит інформації про інші IP адреси Cisco DNS серверів

```
┌──(kali㉿Kali)-[~]
└─$ whois 64.102.255.44
┌──(kali㉿Kali)-[~]
└─$ whois 173.37.145.84
```

Вивід:
NetRange: 72.163.0.0 - 72.163.255.255
CIDR: 72.163.0.0/16
NetName: CISCO-GEN-7
NetHandle: NET-72-163-0-0-1
Parent: NET72 (NET-72-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS109
Organization: Cisco Systems, Inc. (CISCOS-2)

OrgName: Cisco Systems, Inc.
OrgId: CISCOS-2
Address: 170 West Tasman Drive
City: San Jose
StateProv: CA
PostalCode: 95134
Country: US
Питання: Який діапазон IP адрес для IPv4 адрес, виділених Cisco? Сервер ns1.cisco.com адресується в цьому блоці.
Відповідь:

Діапазон IP адрес: 72.163.0.0 - 72.163.255.255
CIDR нотація: 72.163.0.0/16
Це означає, що Cisco має виділений блок з 65,536 IPv4 адрес (весь /16 блок).
Частина 3: Порівняння виводу інструментів nslookup та dig
Крок 1: Використання Linux dig для запиту DNS серверів

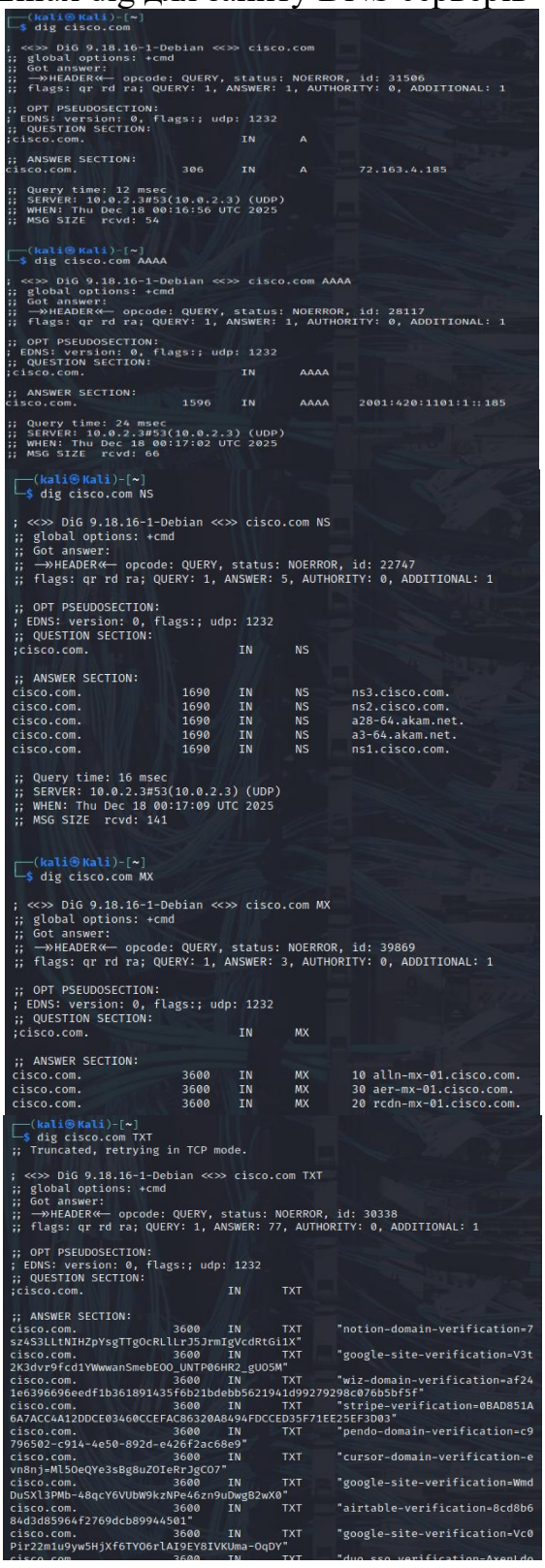

Рис. 8-10. Приклади використання Linux dig.

 # Базовий запит (за замовчуванням запитує A записи)

 # Запит IPv6 адреси (AAAA запис)
 # Запит NS записів
 # Запит MX записів
 # Запит TXT записів

Питання: Яка різниця між типами записів за замовчуванням, які запитує Dig, та тими, які запитує nslookup?

Відповідь:

dig:

За замовчуванням запитує **тільки A записи** (IPv4 адреси)

Для отримання AAAA записів (IPv6) потрібно явно вказати тип запису

nslookup:

За замовчуванням запитує **обидва A та AAAA записи** (і IPv4, і IPv6 адреси)

Повертає обидві версії IP адрес одночасно

Крок 2: Використання dig для отримання додаткової інформації

Команди для dig з конкретним DNS сервером:

 # Запит NS записів через Google DNS (8.8.8.8)

Синтаксис: dig [hostname] @[DNS server IP] [type]

```
┌──(kali㉿Kali)-[~]
└─$ dig cisco.com @8.8.8.8 ns
```

 # Запит ANY записів

```
┌──(kali㉿Kali)-[~]
└─$ dig skillsforall.com any
```

 # Запит через конкретний DNS сервер з типом

```
┌──(kali㉿Kali)-[~]
└─$ dig skillsforall.com @8.8.8.8 any
```

Вивід dig:

```
; <<>> DiG 9.18.8-1-Debian <<>> cisco.com @8.8.8.8 ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62945
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;cisco.com.                     IN      NS

;; ANSWER SECTION:
cisco.com.              1493    IN      NS      ns3.cisco.com.
cisco.com.              1493    IN      NS      ns1.cisco.com.
cisco.com.              1493    IN      NS      ns2.cisco.com.

;; Query time: 83 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
```

;; WHEN: Fri Mar 03 21:15:13 UTC 2023
;; MSG SIZE rcvd: 92

Питання: Порівняйте вивід інструменту dig з виводом nslookup для типу запису any. Який вивід легше читати для отримання значень, що містяться в різних типах записів?

Відповідь:

dig:

Надає більш структурований та детальний вивід
Чітко розділяє секції: QUESTION, ANSWER, AUTHORITY, ADDITIONAL
Показує додаткову технічну інформацію (flags, query time, TTL значення)
Краще підходить для технічного аналізу та автоматизації
Вивід оптимізований для парсингу скриптами

nslookup:

Надає більш простий та читабельний вивід
Менше технічних деталей
Легше для швидкого ручного аналізу
Краще підходить для початківців

Висновок: Для ручного читання **nslookup є легшим**, але для детального технічного аналізу та скриптування **dig надає більш корисну інформацію**.

Частина 4: Виконання зворотних DNS запитів (Reverse DNS Lookups)

Крок 1: Використання dig для виконання rDNS запитів

Команди для зворотних DNS запитів за допомогою dig:

 # Зворотний запит для IP адреси (опція -x)

```
┌──(kali㉿Kali)-[~]
└─$ dig -x 72.163.5.201
```

 # Зворотний запит для іншої IP адреси в тій же підмережі

```
┌──(kali㉿Kali)-[~]
└─$ dig -x 72.163.1.1
```

 # Зворотний запит з конкретним DNS сервером

```
┌──(kali㉿Kali)-[~]
└─$ dig -x 72.163.5.201 @8.8.8.8
```

Вивід:

```
; <<>> DiG 9.18.8-1-Debian <<>> -x 72.163.5.201
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45678
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;201.5.163.72.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
201.5.163.72.in-addr.arpa. 86400 IN    PTR     ns1.cisco.com.
;; Query time: 45 msec
```

;; SERVER: 192.168.1.1#*53(192.168.1.1)*
;; WHEN: Fri Mar 03 22:30:15 UTC 2023
;; MSG SIZE rcvd: 78

Питання: Який тип запису повертається з іменем хоста?

Відповідь:

PTR (Pointer Record) - це тип запису, який повертається при зворотному DNS запиті. PTR запис зіставляє IP адресу з доменним іменем (протилежно до A запису, який зіставляє доменне ім'я з IP адресою).

Питання: Вивчіть вивід команди dig. Який тип пристрою, на вашу думку, має призначену адресу 72.163.1.1?

Відповідь:

На основі типових конвенцій іменування та того, що адреса закінчується на .1, це швидше за все:

Маршрутизатор шлюзу (Gateway Router) або

HSRP віртуальна IP адреса (Hot Standby Router Protocol)

Адреси, що закінчуються на .1 у підмережі, зазвичай резервуються для шлюзових пристроїв або віртуальних IP адрес для забезпечення високої доступності. Якщо у виводі ім'я містить "hsrp" або "gw" (gateway), це підтверджує таку інтерпретацію.

Крок 2: Використання утиліти Host для виконання rDNS запитів

Команди для використання host:

 # Зворотний запит IP адреси

```
┌──(kali㉿Kali)-[~]
└─$ host 72.163.10.1
```

 # Прямий запит доменного імені

```
┌──(kali㉿Kali)-[~]
└─$ host hsrp-72-163-10-1.cisco.com
```

 # Запит для отримання всіх типів записів

```
┌──(kali㉿Kali)-[~]
└─$ host -a cisco.com
```

 # Запит конкретного типу запису

```
┌──(kali㉿Kali)-[~]
└─$ host -t MX cisco.com
```

 # Запит через конкретний DNS сервер

```
┌──(kali㉿Kali)-[~]
└─$ host cisco.com 8.8.8.8
```

Вивід:

 # Зворотний запит

```
┌──(kali㉿Kali)-[~]
└─$ host 72.163.10.1
1.10.163.72.in-addr.arpa domain name pointer hsrp-72-163-10-1.cisco.com.
```

 # Прямий запит

```
┌──(kali㉿Kali)-[~]
└─$ host hsrp-72-163-10-1.cisco.com
```

hsrp-72-163-10-1.cisco.com has address 72.163.10.1

Питання: Як вивід команди host відрізняється від dig або nslookup при запиті IP адреси, призначеної відомому хосту?

Відповідь:

host:

Надає **найкоротший та найпростіший вивід**

Показує тільки основну інформацію без додаткових деталей

Одна лінія результату для простих запитів

Відсутня технічна інформація (TTL, flags, query time)

Найкраще для швидких запитів

dig:

Надає **найдетальніший вивід** з технічною інформацією

Структурований формат з різними секціями

Показує TTL, flags, час запиту, розмір повідомлення

Краще для технічного аналізу

nslookup:

Надає **середній рівень деталізації**

Показує сервер, який відповів на запит

Вказує, чи є відповідь авторитетною

Баланс між простотою та інформативністю

Висновок: host є найшвидшим для простих запитів, **dig** - для детального аналізу, **nslookup** - для інтерактивної роботи.

Команди для запиту aliases (www):

 # Запит www субдомену

```
┌──(kali㉿Kali)-[~]
└─$ host www.cisco.com
```

Вивід:

```
www.cisco.com is an alias for www.cisco.com.akadns.net.
www.cisco.com.akadns.net is an alias for wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net is an alias for e2867.dsca.akamaiedge.net.
e2867.dsca.akamaiedge.net has address 23.50.35.34
```

Цей вивід показує ланцюжок CNAME записів (aliases), що вказує на використання CDN (Content Delivery Network) Akamai для хостингу веб-сайту Cisco.

Крок 3: Використання nslookup для виконання rDNS запитів

Команди для зворотних запитів з nslookup:

 # Неінтерактивний режим (однорядкова команда)

```
┌──(kali㉿Kali)-[~]
└─$ nslookup 72.163.5.201
```

 # Інтерактивний режим

```
┌──(kali㉿Kali)-[~]
└─$ nslookup
> 72.163.5.201
> exit
```

Вивід:

```
┌──(kali㉿Kali)-[~]
└─$ nslookup 72.163.5.201
Server:         192.168.1.1
Address:        192.168.1.1#53
Non-authoritative answer:
201.5.163.72.in-addr.arpa       name = ns1.cisco.com.
Authoritative answers can be found from:
```

Додаткові корисні команди nslookup:

 # Зміна типу запису в інтерактивному режимі

```
┌──(kali㉿Kali)-[~]
└─$ nslookup
> set type=ptr
> 72.163.5.201
```

 # Використання конкретного DNS сервера для зворотного запиту

```
> server 8.8.8.8
> 72.163.5.201
```

Порівняльна таблиця DNS інструментів

ХАРАКТЕРИСТИКА	**NSLOOKUP**	**DIG**	**HOST**
Режим роботи	Інтерактивний та неінтерактивний	Тільки неінтерактивний	Тільки неінтерактивний
Детальність виводу	Середня	Висока (найдетальніший)	Низька (найпростіший)
Типи записів за замовчуванням	A та AAAA	Тільки A	Залежить від запиту
Технічна інформація	Базова	Повна (TTL, flags, timing)	Мінімальна
Легкість використання	Висока	Середня	Дуже висока
Підходить для	Інтерактивної роботи	Скриптування та аналізу	Швидких запитів
Доступність	Linux та Windows	Переважно Linux	Переважно Linux
Формат виводу	Читабельний текст	Структурований формат	Одна лінія

Reflection (Рефлексія)

Питання: У цій лабораторній роботі ви використовували nslookup, dig та host для отримання інформації з файлів зон DNS. Який інструмент ви б використали для початку пасивної розвідки проти цільового домену? Чому?

Відповідь:

Для початку пасивної розвідки проти цільового домену я б рекомендував використовувати **dig** з наступних причин:

Переваги dig:

Детальність інформації: dig надає найбільш повну технічну інформацію, включаючи TTL значення, flags, додаткові секції (ADDITIONAL, AUTHORITY), що допомагає краще зрозуміти конфігурацію DNS.

Гнучкість запитів: dig дозволяє легко запитувати будь-які типи записів (A, AAAA, MX, NS, TXT, SOA, ANY) та використовувати різні DNS сервери для перевірки інформації.
Автоматизація: Формат виводу dig легко парситься скриптами, що дозволяє автоматизувати процес збору інформації.
Стандартизація: dig є стандартним інструментом у Linux/Unix середовищах та широко використовується професіоналами.
Робочий процес пасивної розвідки з dig:

```
# 1. Почати з базового запиту
dig example.com
# 2. Знайти name servers
dig example.com NS
# 3. Знайти mail servers
dig example.com MX
# 4. Шукати TXT записи (SPF, DKIM, verification codes)
dig example.com TXT
# 5. Отримати всю доступну інформацію
dig example.com ANY
# 6. Перевірити SOA запис для інформації про зону
dig example.com SOA
# 7. Спробувати transfer зони (зазвичай не дозволено)
dig example.com AXFR
# 8. Виконати зворотні запити для знайдених IP адрес
dig -x [IP_ADDRESS]
```

Комбінований підхід:
На практиці найефективніше використовувати **комбінацію інструментів**:
dig - для детального технічного аналізу DNS записів
whois - для інформації про реєстрацію домену та IP блоки
host - для швидких перевірок окремих записів
nslookup - для інтерактивного дослідження (якщо потрібно)
Це забезпечує найбільш повний огляд цільового домену без активної взаємодії з цільовою системою.

Висновок
У ході виконання лабораторної роботи було досліджено три основні інструменти DNS розвідки: nslookup, dig та host. Кожен інструмент має свої переваги - nslookup зручний для інтерактивної роботи, dig надає найбільш детальну технічну інформацію та підходить для автоматизації, а host забезпечує швидкі та прості запити. Було отримано практичні навички виконання прямих та зворотних DNS запитів, використання команди whois для визначення IP діапазонів та реєстраційної інформації, а також розуміння різних типів DNS записів (A, AAAA, NS, MX, TXT, PTR, SOA). Ці методи пасивної розвідки є критично важливими для початкового етапу тестування на проникнення, оскільки дозволяють зібрати значну кількість інформації про цільову організацію без прямої взаємодії з її системами.