

DNS LOOKUP



Deborah Binyanya
binyanyadebby@gmail.com

3.1.9 Lab - DNS Lookups

Objectives

Passive reconnaissance is a method of information gathering in which the tools do not interact directly with the target device or network. In this lab, you will explore common tools used to gather information about a target through the Domain Name System (DNS).

- Use **nslookup** to obtain domain and IP address information.
- Use the **whois** command to find additional registration information.
- Compare the Output of the Nslookup and Dig tools.
- Perform Reverse DNS Lookups.

Background / Scenario

Before beginning any penetration test or other ethical hacking engagement, you need to covertly obtain as much information about the target organization as possible. There is a wealth of information that can be obtained from publicly available domain registration data. In this lab, you will investigate the output of the **nslookup**, **whois**, and **dig** commands.

Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

Instructions

Part 1: Use nslookup to Obtain Domain and IP Address Information.

Step 1: Log into Kali Linux and access the terminal environment.

- a. Log into the Kali system with the username **kali** and the password **kali**. You are presented with the Kali desktop.
- b. Open a terminal window by clicking on the **Terminal** icon located near the top of the screen.

Step 2: Investigating nslookup capabilities

Nslookup is a command line tool that is available in Linux and Windows. Its basic usage is to convert a domain name to an IP address. Nslookup has other functionality that can provide additional information.

- a. Access the manual pages for **nslookup** using the **man** command: **man nslookup**
- b. To review the manual pages, press the **spacebar** to advance the pages. When you are finished reviewing the manual pages, press **q** to quit and return to the command line.

NAME

nslookup - query Internet name servers interactively

SYNOPSIS

nslookup [-option] [name | -] [server]

DESCRIPTION

nslookup is a program to query Internet domain name servers. **nslookup** has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Non-interactive mode prints just the name and requested information for a host or domain.

ARGUMENTS

Interactive mode is entered in the following cases:

- a. when no arguments are given (the default name server is used);
- b. when the first argument is a hyphen (-) and the second argument is the host name or Internet address of a name server.

Non-interactive mode is used when the name or Internet address of the host to be looked up is given as the first argument. The optional second argument specifies the host name or address of a name server.

Options can also be specified on the command line if they precede the arguments and are prefixed with a hyphen. For example, to change the default query type to host information, with an initial timeout of 10 seconds, type:

```
nslookup -query=hinfo -timeout=10
```

The **-version** option causes **nslookup** to print the version number and immediately exit.

INTERACTIVE COMMANDS**host [server]**

This command looks up information for **host** using the current default server or using **server**, if specified. If **host** is an Internet address and the query type is A or PTR, the name of the host is returned. If **host** is a name and does not have a trailing period (.), the search list is used to qualify the name.

To look up a host not in the current domain, append a period to the name.

server domain | lserver domain

These commands change the default server to **domain**; **lserver** uses the initial server to look up information about **domain**, while **server** uses the current default server. If an authoritative answer cannot be found, the names of servers that might have the answer are returned.

root This command is not implemented.

finger This command is not implemented.

ls This command is not implemented.

Manual page nslookup(1) line 1 (press h for help or q to quit)

**Step 3: Using the nslookup command**

- a. Use the **nslookup** command with no options to enter interactive mode. To exit interactive mode at any time, type **exit** to return to the CLI prompt.
- b. The CLI prompt changes to > to indicate that you are now in interactive mode and can enter the various nslookup commands. Enter the domain name **cisco.com** to resolve the domain name to an IP address. By default, the **nslookup** command queries A and AAAA records for the target.

The output of the command will be similar to that shown. The A record contains the IPv4 address assigned to the root domain and the AAAA record contains the IPv6 address.

```
Session Actions Edit View Help

(cygieh@kali)-[~]
$ nslookup
> cisco.com
Server:          192.168.221.125
Address:         192.168.221.125#53

Non-authoritative answer:
Name:   cisco.com
Address: 72.163.4.185
Name:   cisco.com
Address: 2001:420:1101:1::185
> █
```

To find the domain name servers configured for cisco.com, use the **set type** command to change the query type to “ns” to return the name server information.

The output of the command should be similar to that shown below. The servers are listed by fully qualified domain name and are further listed as authoritative servers for both IPv4 and IPv6 addresses.

```
> set type=ns
> cisco.com
Server:          192.168.221.125
Address:         192.168.221.125#53

Non-authoritative answer:
cisco.com      nameserver = ns3.cisco.com.
cisco.com      nameserver = a28-64.akam.net.
cisco.com      nameserver = a3-64.akam.net.
cisco.com      nameserver = ns1.cisco.com.
cisco.com      nameserver = ns2.cisco.com.

Authoritative answers can be found from:
> █
```

Step 4: Change the server used to perform lookups.

Occasionally it is desirable to use a different DNS server to perform lookups. This may be necessary if the local DNS server is unable to resolve an address or resolves the host name to an internal private address and you need to obtain the internet accessible address of the host.

- a. In this query, use the one-line **nslookup** command syntax to change the server to look up netacad.com. The syntax for the command is **nslookup [hostname] [server IP]**.

```
(cygieh@kali)-[~]  
$ nslookup netacad.com 8.8.8.8  
Server:      8.8.8.8  
Address:     8.8.8.8#53  
  
Non-authoritative answer:  
Name:   netacad.com  
Address: 52.73.170.64  
Name:   netacad.com  
Address: 44.206.106.175
```

```
(cygieh@kali)-[~]  
$
```

In interactive mode, you change the server using the **server** keyword.

```
(cygieh@kali)-[~]  
$ nslookup  
> server 8.8.8.8  
Default server: 8.8.8.8  
Address: 8.8.8.8#53  
> netacad.com  
Server:      8.8.8.8  
Address:     8.8.8.8#53  
  
Non-authoritative answer:  
Name:   netacad.com  
Address: 52.73.170.64  
>
```

The **any** query type can retrieve much, or all, of the information contained in the DNS record for a host name. Often **text** records that can provide additional details about the domain are contained in DNS records. Using the 8.8.8.8 Google DNS server, find the DNS records for netacad.com.

```

(cygieh@kali)-[~]
$ nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=any
> netacad.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   netacad.com
Address: 52.73.170.64
Name:   netacad.com
Address: 44.206.106.175
netacad.com      nameserver = ns-240.awsdns-30.com.
netacad.com      nameserver = ns-1911.awsdns-46.co.uk.
netacad.com      nameserver = ns-1476.awsdns-56.org.
netacad.com      nameserver = ns-748.awsdns-29.net.
netacad.com
      origin = ns-1476.awsdns-56.org
      mail addr = awsdns-hostmaster.amazon.com
      serial = 1
      refresh = 7200
      retry = 900
      expire = 1209600
      minimum = 86400
netacad.com      mail exchanger = 20 alt2.aspmx.l.google.com.
netacad.com      mail exchanger = 10 aspmx.l.google.com.
netacad.com      mail exchanger = 20 alt1.aspmx.l.google.com.
netacad.com      mail exchanger = 30 aspmx2.googlemail.com.
netacad.com      mail exchanger = 30 aspmx3.googlemail.com.
netacad.com      text = "03hd7nffv5d7h3vbwrc14q6n5cjkjbc2"
netacad.com      text = "identrust_validate=6HH1lQD22HMNen8L8V2*96QqwXOWYA8Y7Tu58KT1JnGv"
netacad.com      text = "google-site-verification=g7CVgKXjcGaa02xXIzPkst9HPpA9_LY0_Uab0_DRTgc"
netacad.com      text = "v=spf1 include:_spf.google.com include:amazonses.com ~all"
netacad.com      text = "facebook-domain-verification=9a8xflw2lo4qxwm9cq3rk3d0etc8bu"
netacad.com      text = "google-site-verification=TxuIwljruI4G9oKael5KB7LvXjIRJg2v0iy8Rky02Ak"
netacad.com      text = "5c9ty312qz1q7yyvly7mmk11nrfpp6kn"

Authoritative answers can be found from:
>

```


Part 2: Use the Whois function to obtain domain information

The whois tool queries domain registration information, rather than the DNS server records. It is another form of passive reconnaissance that can identify where the domain is registered, technical and administrative contact information, and physical locations. Be aware that information contained in domain registrations can be set to private and often the contact information is that of the hosting service, rather than the organization itself.

Step 1: Compare whois output for various organizations.

- a. The whois tool is available from the CLI prompt on Kali Linux. Use the **whois** command to obtain information about cisco.com.

```
(cygneh@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#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
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
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-12-13T18:54:24Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
```

Now use the **whois** command to obtain information about the netacad.com domain.

```
(cygieh@kali)-[~]
$ whois netacad.com
Domain Name: NETACAD.COM
Registry Domain ID: 2667618_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2025-11-04T09:49:03Z
Creation Date: 1998-12-07T05:00:00Z
Registry Expiry Date: 2026-12-06T05:00:00Z
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#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS-1476.AWSDNS-56.ORG
Name Server: NS-1911.AWSDNS-46.CO.UK
Name Server: NS-240.AWSDNS-30.COM
Name Server: NS-748.AWSDNS-29.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-12-13T18:56:27Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
```

Step 2: Use whois to determine IP address registration information.

The whois tool can also be used to gather information about IP address ranges that are assigned to an organization. In the previous part of this lab, we discovered the IP addresses assigned to various domain DNS server host names. Now you can use that address information to obtain additional details about the external IP address ranges that are assigned to those organizations.

- Review the output you obtained from using **nslookup** to obtain the DNS server IP addresses for `cisco.com`. Record the IP addresses of the Cisco DNS servers.
- Use the Whois tool to find what IP address ranges are assigned to Cisco and are used on the networks hosting their DNS servers. At the time of this lab, `ns1.cisco.com` resolved to the IP address `72.163.5.201`, however this may vary. At the prompt, enter **whois 72.163.5.201**.

[illegible]

Because organizations may use the same IP networks for other externally facing servers, knowing the address ranges is valuable for determining which networks to target during a penetration test. Use the whois tool to obtain the IP address allocations for the IP networks where the other Cisco DNS servers are located.

Part 3: Compare the Output of the Nslookup and Dig Functions

Step 1: Use Linux Dig to Query for DNS servers.

- a. Dig is a Linux function that performs DNS queries. The format of a Dig query is similar to that of Nslookup. To resolve the hostname `cisco.com` to an IP address, use the syntax **dig** [hostname].

```

(cygieh@kali)-[~]
$ dig cisco.com

; <<>> DiG 9.20.15-2-Debian <<>> cisco.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 42039
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
cisco.com.                219     IN      A      72.163.4.185

;; Query time: 247 msec
;; SERVER: 192.168.221.125#53(192.168.221.125) (UDP)
;; WHEN: Sat Dec 13 22:02:13 EAT 2025
;; MSG SIZE rcvd: 43

(cygieh@kali)-[~]
$ 

```

To obtain the IPv6 address of cisco.com it is necessary to add a type to the command structure. The syntax to instruct Dig to query a specific record type is **dig [hostname] [record type]**.

```

(cygieh@kali)-[~]
$ dig cisco.com AAAA

; <<>> DiG 9.20.15-2-Debian <<>> cisco.com AAAA
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 47830
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
cisco.com.                95      IN      AAAA    2001:420:1101:1::185

;; Query time: 35 msec
;; SERVER: 192.168.221.125#53(192.168.221.125) (UDP)
;; WHEN: Sat Dec 13 22:04:17 EAT 2025
;; MSG SIZE rcvd: 55

(cygieh@kali)-[~]
$ 

```

Step 2: Use Dig to Obtain Additional Information.

- In the earlier part of this lab, nslookup was used to obtain the DNS servers for cisco.com. Use the 8.8.8.8 Google DNS server to query for the DNS server records. The syntax to use a dig command to perform a query using a different DNS server is **dig [hostname] @[DNS server IP] [type]**. At the prompt, enter **dig cisco.com 8.8.8.8 ns**.

```

(cygieh@kali)-[~]
$ dig cisco.com 8.8.8.8 ns

; <<> DiG 9.20.15-2-Debian <<> cisco.com 8.8.8.8 ns
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 37105
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
cisco.com.                5       IN      A      72.163.4.185

;; Query time: 0 msec
;; SERVER: 192.168.221.125#53(192.168.221.125) (UDP)
;; WHEN: Sat Dec 13 22:05:46 EAT 2025
;; MSG SIZE rcvd: 43

;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NXDOMAIN, id: 32395
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;8.8.8.8.                IN      NS

;; AUTHORITY SECTION:
.                8183    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 20251213
01 1800 900 604800 86400

;; Query time: 43 msec
;; SERVER: 192.168.221.125#53(192.168.221.125) (UDP)
;; WHEN: Sat Dec 13 22:05:47 EAT 2025
;; MSG SIZE rcvd: 111

(cygieh@kali)-[~]
$

```

Part 4: Perform Reverse DNS Lookups Step 1: Use Dig to Perform rDNS Lookups

Now that you can perform DNS lookups and use Whois to determine IP address ranges, use Dig to find additional host names. Reverse DNS (rDNS) lookups use the IP address to query for the host names of the services that resolve to that address.

- a. Enter the **dig** command using the -x option to retrieve the hostname and record type of the ns1.cisco.com DNS server (**72.163.5.201**).

```

(cygieh@kali)-[~]
$ dig -x 72.163.5.201

; <<>> DiG 9.20.15-2-Debian <<>> -x 72.163.5.201
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 49755
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;201.5.163.72.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
201.5.163.72.in-addr.arpa. 600 IN      PTR      ns1.cisco.com.

;; Query time: 236 msec
;; SERVER: 192.168.221.125#53(192.168.221.125) (UDP)
;; WHEN: Sat Dec 13 22:08:52 EAT 2025
;; MSG SIZE rcvd: 81

(cygieh@kali)-[~]
$

```

Use the **dig -x** command to query for another IP address in the same subnet.

```

(cygieh@kali)-[~]
$ dig -x 72.163.1.1

; <<>> DiG 9.20.15-2-Debian <<>> -x 72.163.1.1
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 53141
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;1.1.163.72.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
1.1.163.72.in-addr.arpa. 1800 IN      PTR      hsrp-72-163-1-1.cisco.com.

;; Query time: 844 msec
;; SERVER: 192.168.221.125#53(192.168.221.125) (UDP)
;; WHEN: Sat Dec 13 22:09:59 EAT 2025
;; MSG SIZE rcvd: 91

(cygieh@kali)-[~]
$

```

Step 2: Use the Host Utility to Perform rDNS Lookups

The Host utility is a function in Linux that performs lookups to convert IP addresses to host names. Use this utility to find another host on the 72.163.0.0/16 network.

- a. The syntax of the **host** command is **host [ip address or hostname]**

```

(cygieh@kali)-[~]
$ host 72.163.1.1
1.1.163.72.in-addr.arpa domain name pointer hsrp-72-163-1-1.cisco.com.

```

Host can also be used to perform a quick IP address lookup for a known hostname.


```
(cygieh@kali)-[~]  
$ host hsrp-72-163-1-1.cisco.com  
hsrp-72-163-1-1.cisco.com has address 72.163.1.1  
  
(cygieh@kali)-[~]  
$
```

URLs often contain aliases for the host name of the server hosting the website. The output of the host command can list the servers that respond to that URL.

The information about aliases is useful when trying to determine where the actual website or service is located.

Step 3: Use nslookup to Perform rDNS Lookups

Nslookup is used primarily to perform IP address lookups for known host names. It can also be used to perform rDNS lookups to return a host name assigned to a known IP address.

Use Nslookup to find hostnames associated with an IP address.

In non-interactive mode the syntax to do an rDNS query is nslookup [ip address].

```
(cygieh@kali)-[~]  
$ nslookup 72.163.5.201  
201.5.163.72.in-addr.arpa      name = ns1.cisco.com.  
  
Authoritative answers can be found from:  
  
(cygieh@kali)-[~]  
$
```

To use interactive mode, enter **nslookup** with no options. At the > prompt, enter the target IP address.

```
(cygieh@kali)-[~]  
$ nslookup  
> 72.163.5.201  
201.5.163.72.in-addr.arpa      name = ns1.cisco.com.  
  
Authoritative answers can be found from:  
>
```

