

Lab 3 - 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

- A VM with **nslookup**, **whois**, and **dig** tools installed
- Internet access
- Visit <https://phoenixnap.com/kb/dig-windows> for help with installing Dig on Windows (Alternatively, use Windows Subsystem for Linux)

Instructions

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

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

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

Step 2: Investigating nslookup capabilities

Lab 3 - DNS Lookups

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.

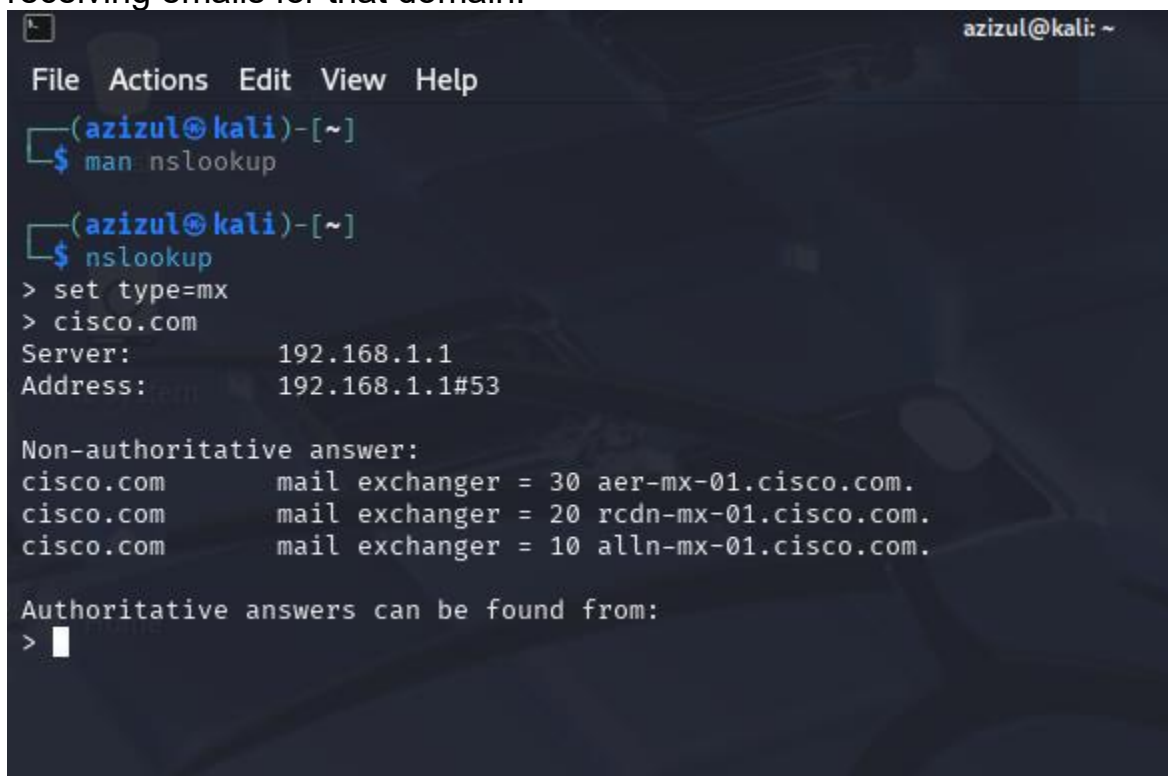
- Access the manual pages for **nslookup** using the **man** command:

```
(kali㉿kali) - [~]  
$ man nslookup
```

- 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.

Which set keyword would you use to query for the mail server mx record within a domain?

Answer: set type=mx, keyword is used to query the mail exchanger (MX) records within a domain. This record identifies the mail servers responsible for receiving emails for that domain.



```
File Actions Edit View Help  
(azizul㉿kali) - [~]  
$ man nslookup  
  
(azizul㉿kali) - [~]  
$ nslookup  
> set type=mx  
> cisco.com  
Server:          192.168.1.1  
Address:         192.168.1.1#53  
  
Non-authoritative answer:  
cisco.com       mail exchanger = 30 aer-mx-01.cisco.com.  
cisco.com       mail exchanger = 20 rcdn-mx-01.cisco.com.  
cisco.com       mail exchanger = 10 alln-mx-01.cisco.com.  
  
Authoritative answers can be found from:  
> 
```

Step 3: Using the nslookup command

- 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.

Lab 3 - DNS Lookups

- 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.

> **cisco.com**

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.

```
(kali㉿Kali)-[~]
└─$ nslookup
> cisco.com
Server:          192.168.1.1
Address:         192.168.1.1#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.

```
> set type=ns
> cisco.com
```

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
;; communications error to 192.168.1.1#53: timed out
Server:          192.168.1.1
Address:         192.168.1.1#53
```

Non-authoritative answer:

```
cisco.com      nameserver = ns1.cisco.com.
cisco.com      nameserver = ns3.cisco.com.
cisco.com      nameserver = ns2.cisco.com.
```

Authoritative answers can be found from:

```
ns2.cisco.com  internet address = 64.102.255.44
<output omitted>
```

Lab 3 - DNS Lookups

What are the IPv4 and IPv6 addresses of the primary DNS server (ns1)?

Answer: Based on the nslookup command results:

```
(azizul@kali)-[~]
$ nslookup
> set type=a
Server: 192.168.1.1
Address: 192.168.1.1#53
Non-authoritative answer:
Name: ns1.cisco.com
Address: 72.163.5.201
> set type=aaaa
Server: 192.168.1.1
Address: 192.168.1.1#53
Non-authoritative answer:
Name: ns1.cisco.com
Address: 2001:420:1101:6::a
>
```

- **IPv4:** 72.163.5.201
- **IPv6:** 2001:420:1101:6::a

- Enter **exit** to leave interactive mode and return to the CLI prompt.

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.

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

```
(kali@Kali)-[~]
$ nslookup skillsforall.com 8.8.8.8
```

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

```
(kali@Kali)-[~]
```

Lab 3 - DNS Lookups

```
└─$ nslookup
> server 8.8.8.8
> skillsforall.com
```

- 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 skillsforall.com.

```
└─(kali㉿Kali)-[~]
└─$ nslookup
> server 8.8.8.8
> set type=any
> skillsforall.com
```

The output should look similar to this example:

```
└─(kali㉿Kali)-[~]
└─$ nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> 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: 13.225.142.127
Name:    skillsforall.com
Address: 13.225.142.7
Name:    skillsforall.com
Address: 13.225.142.73
Name:    skillsforall.com
Address: 13.225.142.9
skillsforall.com      nameserver = ns-1130.awsdns-13.org.
skillsforall.com      nameserver = ns-1652.awsdns-
14.co.uk.
skillsforall.com      nameserver = ns-489.awsdns-61.com.
skillsforall.com      nameserver = ns-588.awsdns-09.net.
skillsforall.com
origin = ns-1130.awsdns-13.org
mail addr = awsdns-hostmaster.amazon.com
```

Lab 3 - DNS Lookups

```
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 =
"d1g1l19y74sxj8m.cloudfront.net"
skillsforall.com      text = "facebook-domain-
verification=8cg08gu4eikp0d2d1quqhjwh5tilvv"
skillsforall.com      text = "google-site-
verification=Q5NIWRygJYTSLxuHReNKw1kvgC8IXKTOyPf5zITDv40"
skillsforall.com      text =
"identrust_validate=tadDBgWwQAKpw6QCCQDCagqsZgxHELybnPOCQHN
U+rsV"
```

What record types are displayed in the output of the nslookup command with the type set to any?

Answer: A, AAAA, NS, SOA, MX, TXT, are displayed in the output of the nslookup command with the type set to any.

Lab 3 - DNS Lookups

```
(azizul@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: 13.226.34.88
Name:   skillsforall.com
Address: 13.226.34.26
Name:   skillsforall.com
Address: 13.226.34.24
Name:   skillsforall.com
Address: 13.226.34.113

(azizul@kali)-[~]
$ nslookup skillsforall.com
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> skillsforall.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   skillsforall.com
Address: 13.226.34.88
Name:   skillsforall.com
Address: 13.226.34.26
Name:   skillsforall.com
Address: 13.226.34.24
Name:   skillsforall.com
Address: 13.226.34.113
> set type=any
> skillsforall.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   skillsforall.com
Address: 3.167.37.25
Name:   skillsforall.com
Address: 3.167.37.22
Name:   skillsforall.com
Address: 3.167.37.99
Name:   skillsforall.com
Address: 3.167.37.33
skillsforall.com      nameserver = ns-1130.awsdns-13.org.
skillsforall.com      nameserver = ns-489.awsdns-61.com.
skillsforall.com      nameserver = ns-1652.awsdns-14.co.uk.
skillsforall.com      nameserver = ns-588.awsdns-09.net.
skillsforall.com      server origin = ns-1130.awsdns-13.org
skillsforall.com      address mail addr = awsdns-hostmaster.amazon.com
skillsforall.com      serial = 1
skillsforall.com      refresh = 7200
skillsforall.com      retry = 900
skillsforall.com      expire = 1209600
skillsforall.com      minimum = 86400
skillsforall.com      mail exchanger = 10 inbound-smtp.us-east-1.amazonaws.com.
skillsforall.com      text = "d1g1l9y74sxj8m.cloudfront.net"
skillsforall.com      text = "google-site-verification=Q5NIWRygJYTSLxuHReNKw1kvgC8IXKT0yPf5zITDv40"
skillsforall.com      text = "v=spf1 include:amazonses.com ~all"
skillsforall.com      text = "facebook-domain-verification=8cg08gu4eikp0d2d1quqhjwh5t11vv"
skillsforall.com      text = "identrust_validate=XzTu3rqoVVwnwNykPpaGYBeA4de5HaSynIEnsHWXyIur"

Authoritative answers can be found from:
>
```

- A records for (IPv4 addresses)

Lab 3 - DNS Lookups

- AAAA records for (IPv6 addresses)
- MX records for (Mail servers)
- NS records for (Name servers)
- TXT records for (Text data)
- SOA for (Start of Authority)

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.

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

```
(kali㉿Kali) - [~]  
$ whois cisco.com
```

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

What conclusion can you make about the two domains (cisco.com and skillsforall.com) based on the output of the whois commands?

Answer:

Cisco.com: Cisco is a globally recognized company. The Whois output will display:

- Registrar: Cisco's official domain registrar.
- Organization: Cisco Systems, Inc.
- Location: Headquarters at 170 West Tasman Drive, San Jose, CA, USA.
- Administrative & Technical Contact Information.
- Network Details (IP ranges assigned to Cisco).

Lab 3 - DNS Lookups

Established presence with historical records.

```
(azizul@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: 2021-04-14T17:05:53Z
Creation Date: 2013-08-27T18:04:50Z
Registry Expiry Date: 2025-08-27T18:04:50Z
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#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
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/wicf/
>>> Last update of whois database: 2025-03-09T17:54:04Z <<<
```

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

skillsforall.com: SkillsForAll.com is likely registered through a cloud provider (e.g., AWS).

Possible Whois Privacy Protection Enabled:

Lab 3 - DNS Lookups

- Limited or hidden registration details.
- Registrar may be Amazon Web Services (AWS) or another cloud-based provider.
- Contact details may show privacy-protected information, meaning real owners are not visible.

Lab 3 - DNS Lookups

- The domain is likely used for an online learning platform, not a corporate entity like Cisco.

Lab 3 - DNS Lookups

```
(azizul@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: 2021-04-14T17:05:53Z
Creation Date: 2013-08-27T18:04:50Z
Registry Expiry Date: 2025-08-27T18:04:50Z
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#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
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/wicf/
>>> Last update of whois database: 2025-03-09T17:54:04Z <<<

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
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
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: 2024-08-02T02:17:33+0000
Creation Date: 2013-08-27T18:04:50+0000
Registrar Registration Expiration Date: 2025-08-27T18:04:50+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Registry Registrant ID:
```

Lab 3 - DNS Lookups

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**.

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

#
# ARIN WHOIS data and services are subject to the Terms of
# Use
# available at:
# https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_re
# porting/
#
# Copyright 1997-2023, American Registry for Internet
# Numbers, Ltd.
#
```

```
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)
RegDate:          2006-10-24
Updated:          2022-06-09
```

Lab 3 - DNS Lookups

Ref:

<https://rdap.arin.net/registry/ip/72.163.0.0>

OrgName: Cisco Systems, Inc.
OrgId: CISCOS-2
Address: 170 West Tasman Drive
City: San Jose
StateProv: CA
PostalCode: 95134
Country: US
RegDate: 1986-02-05
Updated: 2021-10-27

Ref:

<https://rdap.arin.net/registry/entity/CISCOS-2>

OrgTechHandle: CAMT-ARIN
OrgTechName: Cisco address management team
<output omitted>

What is the IP address range for the IPv4 addresses allocated to Cisco? The ns1.cisco.com server is addressed within this block.

Answer: The IPv4 address range allocated to Cisco is:

- IPv4 Range: 72.163.0.0 - 72.163.255.255
- CIDR: 72.163.0.0/16

Lab 3 - DNS Lookups

```
(azizul@kali)-[~]
$ whois 72.163.5.201

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
# server 8.8.8.8
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
# skillstorall.com
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
# Address: 8.8.8.8:53

Non-authoritative answer:
NetRange: skillstorall.com 72.163.0.0 - 72.163.255.255
CIDR: skillstorall.com 72.163.0.0/16
NetName: skillstorall.com CISCO-GEN-7
NetHandle: skillstorall.com NET-72-163-0-0-1
Parent: skillstorall.com NET72 (NET-72-0-0-0-0)
NetType: skillstorall.com Direct Allocation
OriginAS: skillstorall.com AS109
Organization: skillstorall.com CISCO SYSTEMS, INC. (CS-2831)
RegDate: skillstorall.com 2006-10-24
Updated: skillstorall.com 2024-03-08
Comment: skillstorall.com Geofeed https://www.cisco.com/web/automation/CiscoAS109_geoip.csv
Ref: skillstorall.com https://rdap.arin.net/registry/ip/72.163.0.0

Non-authoritative answer:
OrgName: skillstorall.com CISCO SYSTEMS, INC.
OrgId: skillstorall.com CS-2831
Address: skillstorall.com 251 LITTLE FALLS DRIVE
City: skillstorall.com WILMINGTON
StateProv: skillstorall.com DE
PostalCode: skillstorall.com 19808
Country: skillstorall.com US
RegDate: skillstorall.com 2023-06-07
Updated: skillstorall.com 2024-02-16
Ref: skillstorall.com https://rdap.arin.net/registry/entity/CS-2831
nameserver = ns-1130.awsdns-13.org.
nameserver = ns-1652.awsdns-14.co.uk.
nameserver = ns-588.awsdns-09.net.
OrgTechHandle: GATC-ARIN
OrgTechName: skillstorall.com GIS ARIN Technical Contact
OrgTechPhone: skillstorall.com +1-408-526-8888
OrgTechEmail: skillstorall.com cidr-block-admins@cisco.com
OrgTechRef: skillstorall.com https://rdap.arin.net/registry/entity/GATC-ARIN
OrgNOCHandle: GATC-ARIN
OrgNOCName: skillstorall.com GIS ARIN Technical Contact
OrgNOCPhone: skillstorall.com +1-408-526-8888
OrgNOCEmail: skillstorall.com cidr-block-admins@cisco.com
OrgNOCRef: skillstorall.com https://rdap.arin.net/registry/entity/GATC-ARIN
text = "v=spf1 include:amazonses.com ~all"
OrgAbuseHandle: CISC06-ARIN
OrgAbuseName: skillstorall.com Cisco CSIRT
OrgAbusePhone: skillstorall.com +1-408-527-3227
OrgAbuseEmail: skillstorall.com csirt-notify@cisco.com
OrgAbuseRef: skillstorall.com https://rdap.arin.net/registry/entity/CISC06-ARIN
```

Lab 3 - DNS Lookups

Since ns1.cisco.com falls within this range (72.163.5.201), this confirms that Cisco owns and manages this IP block.

This exercise demonstrates how whois can be used for passive reconnaissance to discover IP ranges, ownership details, and network allocations of an organization.

- 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.

- 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].

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

What is the difference between the default record types queried by Dig and those queried by Nslookup?

Answer: Difference Between Nslookup and Dig are:

Nslookup:

- Nslookup queries only for the A record (IPv4 address) of a domain by default.
- It provides a simplified output, showing only the server used and the queried domain's resolved IP.

Lab 3 - DNS Lookups

```
(azizul@kali)-[~]
$ nslookup cisco.com
Server: 192.168.1.1
Address: 192.168.1.1#53
Name Server: NS1.CISCO.COM
Non-authoritative answer:
Name: cisco.com
Address: 72.163.4.185
Name: cisco.com
Address: 2001:420:1101:1::185
For more information on Whois status see
$
```

Dig : Dig retrieves a lot more information than Nslookup. By default, Dig queries for an A record, but its output includes:

- Header information (Query status, flags, etc.)
- Question section (The domain being queried)
- Answer section (IP address resolution)
- Authority section (Authoritative name servers)
- Additional section (Extra DNS information)

Lab 3 - DNS Lookups

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

; <<>> DiG 9.20.4-4-Debian <<>> cisco.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 18582
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cisco.com. IN A

;; ANSWER SECTION:
cisco.com. 1432 IN A 72.163.4.185

;; Query time: 28 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun Mar 09 14:03:23 EDT 2025
;; MSG SIZE rcvd: 54
```

Differences between Nslookup and Dig

Feature	Nslookup	Dig
Default Record Queried	A Record (IPv4)	A Record (IPv4)
Output Format	Simple	Detailed
Additional Sections	No	Yes (Question, Answer, Authority, Additional)
Flexibility	Less flexible	More powerful with multiple query options
Use in Scripts	Limited	Preferred due to structured output

The main difference is that Nslookup provides a simpler output, focusing only on the IP resolution, while Dig provides a detailed breakdown of the DNS query, including authoritative name servers and additional DNS information.

Lab 3 - DNS Lookups

- 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]**.

```
(kali㉿Kali)-[~]  
$ dig cisco.com AAAA
```

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**.

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

```
; <<>> 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
```

```
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 512  
;; QUESTION SECTION:  
;cisco.com.                IN      NS  
  
;; ANSWER SECTION:  
cisco.com.                 1493    IN      NS  
ns3.cisco.com.             1493    IN      NS  
cisco.com.                 1493    IN      NS  
ns1.cisco.com.             1493    IN      NS  
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  
<output omitted>
```

Lab 3 - DNS Lookups

- Earlier, nslookup was used with the **set type=any** option to find additional information about the skillsforall.com hostname. The **any** record type can also be queried using Dig.

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

Compare the output of the Dig function with the output of Nslookup for the *any* record type. Which output is easier to read to obtain the values contained in the various record types?

Answer: When comparing the output of the Dig function and Nslookup for the ANY record type query, the Nslookup output is easier to read because it presents the DNS records in a simplified and direct format, listing each record type without additional technical details. On the other hand, Dig provides a more detailed and structured response, including metadata such as query status, flags, TTL (Time-To-Live), and sections like the question, answer, authority, and additional records. While this makes Dig more powerful for troubleshooting, it can also make it harder to quickly extract the necessary values compared to Nslookup.

For a quick lookup of various DNS record types, Nslookup is easier to read. However, for in-depth analysis and advanced DNS troubleshooting, Dig provides more comprehensive information.

Lab 3 - DNS Lookups

```
(azizul@kali)-[~]
$ dig cisco.com @8.8.8.8 ns
; <<>> DiG 9.20.4-4-Debian <<>> cisco.com @8.8.8.8 ns
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 46022
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cisco.com. VeriSign ) Whois da IN se 1 NS
;; ANSWER SECTION:
cisco.com. 1800 IN NS ns3.cisco.com.
cisco.com. 1800 IN NS ns2.cisco.com.
cisco.com. 1800 IN NS ns1.cisco.com.
;; Query time: 36 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Mar 09 14:25:19 EDT 2025
;; MSG SIZE rcvd: 92

(azizul@kali)-[~]
$ dig skillsforall.com any
; <<>> DiG 9.20.4-4-Debian <<>> skillsforall.com any
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOTIMP, id: 18175
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: EDNS query returned status NOTIMP - retry with '+noedns'
;; QUESTION SECTION:
;skillsforall.com. IN ANY
;; Query time: 40 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (TCP)
;; WHEN: Sun Mar 09 14:28:36 EDT 2025
;; MSG SIZE rcvd: 34
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
UpdateProhibited (https://www.icann.org/epp#clientUpda
StatusClientTransferProhibited (https://www.icann.org/epp#clientTr
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDele
```

Part 4: Perform Reverse DNS Lookups

Lab 3 - 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.

- 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**).

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

What type of record is returned with the host name?

Answer: The record type returned is a PTR (Pointer) record, which resolves the IP address to its corresponding hostname. PTR records are used in reverse DNS lookups to verify the domain name linked to an IP address.

```
(azizul㉿kali) - [~]  
$ dig -x 72.163.5.201  
  
; <<>> DiG 9.20.4-4-Debian <<>> -x 72.163.5.201  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 34566  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:;; udp: 512  
;; 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: 40 msec  
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)  
;; WHEN: Sun Mar 09 14:32:29 EDT 2025  
;; MSG SIZE rcvd: 81  
  
(azizul㉿kali) - [~]  
$
```

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

```
(kali㉿Kali) - [~]
```

Lab 3 - DNS Lookups

```
└─$ dig -x 72.163.1.1
```

Examine the output returned from the dig command. What type of device do you think is assigned the 72.163.1.1 address?

Answer: Based on the IP address range (72.163.0.0/16) assigned to Cisco, and considering that 72.163.1.1 is in the same subnet, this IP is likely assigned to a network device such as a router, firewall, or a Cisco-managed infrastructure service.

```
(azizul@kali)-[~]
└─$ dig -x 72.163.1.1
; <<>> DiG 9.20.4-4-Debian <<>> -x 72.163.1.1
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 20231
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;1.1.163.72.in-addr.arpa.  IN  PTR
1.1.163.72.in-addr.arpa. 1800 IN PTR hsrp-72-163-1-1.cisco.com.

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

;; Query time: 56 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun Mar 09 14:34:37 EDT 2025
;; MSG SIZE rcvd: 91
```

Explanation:

- **HSRP:** HSRP stands for Hot Standby Router Protocol. This is a Cisco proprietary protocol that provides redundancy for IP networks. The presence of "HSRP" in the hostname strongly suggests it's a router using this protocol.
- **Naming Convention:** The hostname follows a pattern typically used by Cisco to identify devices on their network, often including the IP address within the name.

Step 2: Use the Host Utility to Perform rDNS Lookups

Lab 3 - DNS 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.

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

```
(kali㉿kali) - [~]  
└─$ host 72.163.10.1
```
- Host can also be used to perform a quick IP address lookup for a known hostname.

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

How does the output of the host command differ from Dig or Nslookup when querying for an IP address assigned to a known host?

Answer: The `host` command typically provides a simpler, more direct output, showing just the hostname associated with the IP address. `Dig` and `nslookup` provide more detailed information, including record types, server information, and other DNS-related data.

```
(azizul㉿kali) - [~]  
$ host 72.163.10.1  
1.10.163.72.in-addr.arpa domain name pointer hsrp-72-163-10-1.cisco.com.  
  
(azizul㉿kali) - [~]  
$ host hsrp-72-163-10-1.cisco.com  
hsrp-72-163-10-1.cisco.com has address 72.163.10.1  
  
(azizul㉿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.

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

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.

Lab 3 - DNS Lookups

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].

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

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

```
(kali㉿Kali) - [~]  
$ nslookup  
> 72.163.5.201
```

Reflection

In this lab, you used nslookup, dig, and host to obtain information from DNS zone files. Which tool would you use to begin a passive reconnaissance effort against a targeted domain? Why?

Answer: I would use dig to begin a passive reconnaissance effort. Dig offers more detailed and comprehensive information compared to nslookup. It provides greater control over query types and server selection, allowing for targeted and flexible DNS lookups. The additional information that dig provides such as answer, authority, and additional records is extremely valuable during the reconnaissance stage of penetration testing, as it can reveal key details about a target's infrastructure, mail servers, subdomains, and authentication records.