Lab - DNS Lookup

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:

```
┌──(kali㉿Kali)-[~]
└─$ 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.

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

Answer Area

<!----><!---->

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.

```
> 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
>
```

c. 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>
```

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

Answer Area

<!----><!---->

d. 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.

a. 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)-[~]
└─$ nslookup
> server 8.8.8.8
> skillsforall.com
```

b. 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
        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 = "d1g1l9y74sxj8m.cloudfront.net"

   skillsforall.com        text = "facebook-domain-verification=8cg08gu4eikp0d2d1quqhjwh5ti1vv"

   skillsforall.com        text = "google-site-

   verification=Q5NIWRygJYTSLxuHReNKw1kvgC8IXKTOyPf5zITDv40"

   skillsforall.com        text =

   "identrust_validate=tadDBgWwQAKpw6QCCQDCagqsZgxHELybnPOCQHNU+rsV"
```

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

Answer Area

<!----><!---->

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 ion Kali Linux. Use the **whois** command to obtain information about cisco.com.

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

b. 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 Area

<!----><!---->

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.

a. 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.
b. 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_reporting/
#
# 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
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 Area

<!----><!---->

c. 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].

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

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

Answer Area

<!----><!---->

b. 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.

a. 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.
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
<output omitted>
```

b. 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 Area

<!----><!---->

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)**.

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

What type of record is returned with the host name?

Answer Area

<!----><!---->

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

```
┌──(kali㉿Kali)-[~]
└─$ 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 Area

<!----><!---->

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*]

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

b. 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 Area

<!----><!---->

c. 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.

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 Area

<!----><!---->