# Networking Lab 8 DNS

The Domain Name System (DNS) is an essential part of the Internet that maps human readable domain names to IP addresses. The DNS client on your host connects to a DNS server, or resolver, that looks up domain names using the DNS tree structure. In this lab, we’ll emulate the process that a DNS server uses to convert domain names into IP addresses.

## DNS Tools

There are two primary DNS tools that are available on Windows and Linux systems. The older tool is nslookup. It is available on both Windows and Linux, but is deprecated on Linux. The newer tool is dig, which is mainly available on Linux. Nslookup and dig have many options, but we’ll just use the option to specify the DNS server we will query, and the type of DNS record we will ask for.

# NSLOOKUP

We will use nslookup in interactive mode. The commands, set type=ns or set type=a, tell nslookup whether we want name server (NS) or address (A) records. We’ll use the command, server, to select the DNS server we want to query. Otherwise, nslookup will use the DNS server specified in our computer’s IP configuration. Also, note the “dot” at the end of the request for [www.vccs.edu](http://www.vccs.edu)., which tells nslookup that is the entire name we are looking for, or Fully Qualified Domain Name (FQDN). If you don’t do that, your host may add its own domain name to the end. Here is an example:

C:\>nslookup

Default Server: cdns01.comcast.net

Address: 75.75.75.75

> set type=ns

> server 164.106.1.1

Default Server: ns1.vccs.edu

Address: 164.106.1.1

> www.vccs.edu.

Server: ns1.vccs.edu

Address: 164.106.1.1

vccs.edu

primary name server = ns1.vccs.edu

responsible mail addr = alyon.vccs.edu

serial = 458660324

refresh = 1200 (20 mins)

retry = 180 (3 mins)

expire = 1209600 (14 days)

default TTL = 3600 (1 hour)

If a DNS resolver does not have the answer to the query in cache, it starts searching from the root of the DNS tree as shown on the graphic on slide 9 of CyberAces\_Module2-Networking-Layer7\_20150129.pdf. We will follow the same procedure manually, using nslookup or dig.

Let’s use the procedure to look up the IP address of the site of your choice. We’ll call the site you have chosen, www.mysite.tld. Note: [www.svgs.k12.va.us](http://www.svgs.k12.va.us) is complicated, so don’t try that right away. Many .us and .net domains will redirect you to a name server in the .com TLD, so it’s easiest to look for something in the .com domain.

## Query the DNS root

Use a search engine to find the IP address of one of the DNS root servers (search for “dns root server”.)

Query the root server for your site. First set the type of record you want to be a name server record, NS. The set nslookup to query the root name server IP address you found.  
*nslookup  
set type=ns  
server [IP address of root server]*

Then ask for the site you are looking for. Don’t forget the dot at the end.

*mysite.tld.*

You should get the name server IP address for tld.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ TLD nameserver IP address.

## Query the TLD server

Change the server address in nslookup to that you found for the tld, and ask again.

*server [IP address of TLD name server]  
mysite.tld.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ mysite.tld nameserver address

## Repeat as necessary

If you have a long site name, like aaa.bbb.ccc.ddd.com, you may have to do this several times.

## Ask for the final answer

If you are trying to browse to [www.mysite.tld](http://www.mysite.tld), that’s the final answer you are looking for. Now that we know the nameserver IP address for mysite.tld, we need to change from name server (NS) records to address (A) records.

*set type=A  
server [IP address of mysite.tld name server]*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [www.mysite.tld](http://www.mysite.tld) address

## One more thing

The name server you used for your last query is probably an “authoritative” server for the mysite.tld domain. Remember that the CyberAces module says that it is bad security practice to have an authoritative DNS server that also resolves addresses (a recursive DNS server.) Use nslookup to query the server you used for the previous step for a completely different domain than mysite.tld. Does it give you an answer? Note: The Google DNS server is unusual, in that it does resolve names in addition to providing authoritative answers for google.com. Google does this as a service to the community, and has no doubt done extra work to be able to do both securely.

# DIG

Note: dig is only available in Linux, so use your Linux VM.

The format for dig is shown below. “@[IP address]” is the address of the DNS server you want to use for the query. “Type” is the record type you want the server to return. We’ll be using Name Server (NS) and Address (A) records. Slide 7 in the CyberAces module shows you the other possibilities. In the example for nslookup, we queried the server 164.106.1.1 to find the IP address of [www.vccs.edu](http://www.vccs.edu). Here’s what it looks like in dig.

[john@localhost ~]$ dig @164.106.1.1 www.vccs.edu NS

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6\_7.4 <<>> @164.106.1.1 www.vccs.edu NS

; (1 server found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12370

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:

;www.vccs.edu. IN NS

;; AUTHORITY SECTION:

vccs.edu. 3600 IN SOA ns1.vccs.edu. alyon.vccs.edu. 458660325 1200 180 1209600 3600

;; Query time: 13 msec

;; SERVER: 164.106.1.1#53(164.106.1.1)

;; WHEN: Mon Nov 9 15:20:12 2015

;; MSG SIZE rcvd: 76

## Query the DNS root

Use a search engine to find the address of one of the DNS root servers (search for “dns root server”.)

Query the root server for your site. First set the type of record you want to be a name server record, NS. The set nslookup to query the root name server IP address you found.  
*dig @[IP address of root name server] mysite.tld NS*

You should get the name server IP address for tld.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ TLD nameserver IP address.

## Query the TLD server

Change the server address to that you found for the tld, and ask again.

*dig @[IP address of TLD name server] mysite.tld. NS*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ mysite.tld nameserver address

## Repeat as necessary

If you have a long site name, like aaa.bbb.ccc.ddd.com, you may have to do this several times.

## Ask for the final answer

If you are trying to browse to [www.mysite.tld](http://www.mysite.tld), that’s the final answer you are looking for. Now that we know the nameserver IP address for mysite.tld, we need to change from name server (NS) records to address (A) records.

*dig @[IP address of mysite.tld name server]* [*www.mysite.tld*](http://www.mysite.tld) *A*

*note: the default type is dig is the A record, so you can omit the A if you like.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [www.mysite.tld](http://www.mysite.tld) address

## One more thing

The name server you used for your last query is probably an “authoritative” server for the mysite.tld domain. Remember that the CyberAces module says that it is bad security practice to have an authoritative DNS server that also resolves addresses (a recursive DNS server.) Use dig to query the server you used for the previous step for a completely different domain than mysite.tld. Does it give you an answer?

# Reverse (IP address) Lookup in DNS

Organizations will often create PTR records for some of their IP addresses, which point to a DNS name attached to them. This allows you to look up IP addresses and sometimes find a DNS name. For example, at SVGS we can look up the address 172.18.10.40 and find that it is svgs-dc02.svgs.local. This only works if the organization has created a PTR record for the address in their DNS

nslookup

> 172.18.10.40

Server: svgs-dc01.svgs.local

Address: 172.18.10.39

Name: svgs-dc02.svgs.local

Address: 172.18.10.40

# DNS Registration

DNS addresses are purchased through domain registrars, companies that have purchased the rights to add domains to the top-level domains like .com, .org, .net, and the like. They maintain databases of the domains they issue and information about who they issued them to. It is useful to examine this information when you are researching a domain or trying to notify a domain that one of their hosts is attacking you. Often, however, the information is hidden anonymity services.

Malware domains tend to pop up and disappear frequently. A clue that a domain is used for malware may be that it was issued recently, within the last month or so. The issue date for a domain is also available through the registrar.

Registrars maintain servers to respond to queries using the whois protocol. A whois client is normally available in Linux by default. A Windows whois client is available from <https://docs.microsoft.com/en-us/sysinternals/downloads/whois>. You can also obtain whois information using web queries, but a good whois client is usually faster.

## Whois Lab

Download the Windows whois client from the link above. Query several domain names of your choosing. Take note of the date the domain was issued, and whether or not the entry lists contact data.

# IP Address Lookup

It is also useful to see who owns IP addresses, especially if those addresses are attacking you. Regional Internet Registries (RIR) issue IP addresses. The American Registry for Internet Numbers (ARIN) issues addresses for the US. Other registries are RIPE for Europe, APNIC for Asia, LACNIC for Latin America, and AFNIC for Africa. <https://www.arin.net/knowledge/rirs.html>.

## IP Address Lab

The website for ARIN is [www.arin.net](http://www.arin.net). We will use it to check ownership for some IP addresses.

1. Open two or three tabs in your browser to sites of your choosing.
2. Use the command “netstat -na” in the command prompt to see if your computer has ESTABLISHED connections to remote hosts (not 172.18.10.0/23) on ports 80 or 443.
3. Then use the Search Whois feature on the ARIN site to see who owns the IP addresses.

Note: you can eliminate some of the unnecessary information in the netstat output by using  
netstat -na | find “ESTABLISHED” This only works from a command prompt, and does not work in PowerShell.

# Turn In

Turn in (copy/paste or screenshot, your choice) the results of:

1. An nslookup query
2. A whois query
3. An IP address query to ARIN