Networking

Networking Fundamentals

1.6.2 - DNS

What is DNS and and what are the different types of records within a domain?

Overview

The student will explain the use and purpose of network services

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA N10-008 Network+ Objectives

Objective 1.6

- Explain the use and purpose of network services
    - DNS
        - Record Types
            - Address (A vs AAAA)
            - Canonical Name (CNAME)
            - Mail Exchange (MX)
            - Start of Authority (SOA)
            - Pointer (PTR)
            - Text (TXT)
            - Service (SRV)
            - Name server (NS)
        - Global hierarchy
            - Root DNS servers
        - Internal vs. External
        - Zone transfers
        - Authoritative name servers
        - Time to live (TTL)
        - DNS caching
        - Reverse DNS/reverse lookup/forward lookup
        - Recursive lookup/iterative lookup

DNS

Domain Name System

The *DNS, or Domain Name System*, is the service that translates IP addresses to domain names. Thus, users can type in the URL www.google.com instead of 142.251.40.174. While the IP address is the actual address of Google (along with a lot of other IP addresses), it is easier for the average person to remember "google.com" over the 4 numbers for the IP address. This will really come in handy as the internet slowly shifts to IPv6, imagine trying to memorize "http://7727:c1ce:4590:edbc:539a:739e:fe35:a596" as a web address! Once a user types in the URL, a DNS server will translate the URL to the IP address so the correct web server can be located.

Teacher Notes:

The Root Servers

Where is all the DNS records stored? There are billions of websites, each needing their own IP address and domain name, where is all the DNS data stored? It's all controlled by the ***root DNS servers***, in which there are 12 organizations that control these root servers. While ICANN (Internet Corporation for Assigned Names and Numbers) is one of these organizations, they are the authority over top of these DNS servers and the bylaws that control them. Here's a table of the 13 root servers (Lettered A – M), their organization, and how many DNS sites they maintain:

Letter	Organization	Number of Sites (As of March 2022)
A	Verisign	16
B	University of Southern California (ISI)	6
C	Cogent Communications	12
D	University of Maryland	175
E	NASA	254
F	Internet Systems Consortium	302
G	Defense Information System Agency	6
H	US Army	12
I	Netnod	68
J	Verisign	118
K	RIPE NCC	82
L	ICANN	197
M	WIDE Project	8

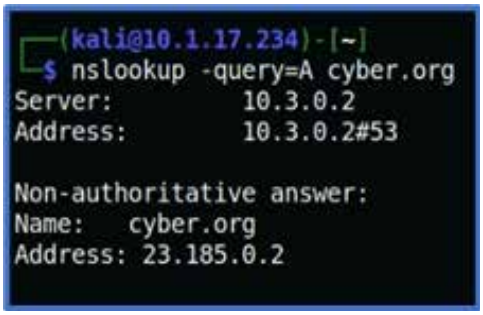
The root-servers website is https://www.root-servers.org and this shows the specific location of the root servers. These root servers are located, and purposefully spread out, across the planet. This is to protect the root servers if something was to happen on one side of the planet but also for ease of access for all locations. These DNS servers are a very important part to the backbone of the internet and have been attacked before, but to this date, no attack has been able to have a significant amount of damage to these servers.

Teacher Notes:

Record Types

What information is stored on these root servers? There is a lot of information stored on these servers, more than just the IP addresses aligned with the domains, here is a list of the types of records stored on a DNS server.

Address (A vs AAAA) - These are the IP addresses of the domain name. "A" is the IPv4 address while "AAAA" is the IPv6 address.

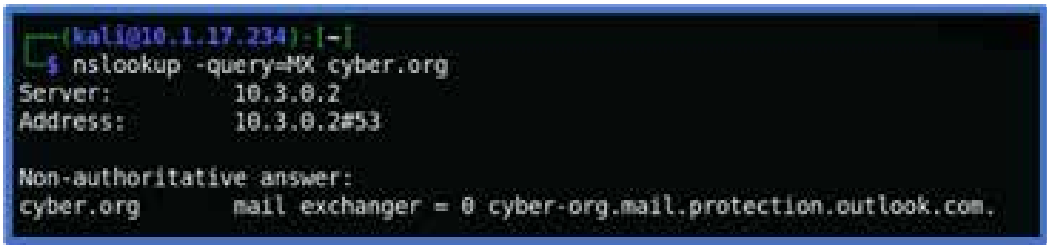


CYBER.ORG's A record

CYBER.ORG's AAAA record

Canonical Name (CNAME) – These are when a domain name is an alias for another domain name. For example, CYBER.ORG used to be known as NICERC, thus if you go to "nicerc.org", it will now redirect you to cyber.org.

Mail exchange (MX) – This is how email messages should be routed for that domain



CYBER.ORG's mail server using Outlook

Teacher Notes:

Start of authority (SOA) - This provides information about the administrator of domain, such as their email address.

```
┌──(kali@10.1.17.234)-[~]
└─$ nslookup -query=SOA cyber.org
Server:         10.3.0.2
Address:        10.3.0.2#53

Non-authoritative answer:
cyber.org
        origin = ns15.domaincontrol.com
        mail addr = dns.jomax.net
        serial = 2022021501
        refresh = 28800
        retry = 7200
        expire = 604800
        minimum = 600
```

Here, dns.jomax.net is what GoDaddy, who controls the domain CYBER.ORG, uses for their administrator email

CYBER.ORG's SOA record

Pointer (PTR) - This returns the domain name, is used for a reverse lookup when someone searches with an IP address instead of a domain name.

Text (TXT) – This was originally meant for administrators to put text as notes for themselves or people using their domain. However, it is now used for machine readable code, as well as authorized IP addresses for servers, and ways to prevent spam emails from reaching the system.

```
┌──(kali@10.1.17.234)-[~]
└─$ nslookup -query=TXT cyber.org
Server:         10.3.0.2
Address:        10.3.0.2#53

Non-authoritative answer:
cyber.org       text = "v=spf1 ip4:66.76.161.60 include:spf.protection.outlook.com -all"
cyber.org       text = "google-site-verification=TY__YSRdbvoIzq8AQezKJPxB79tV-qykxSue5hDL5_E"
```

CYBER.ORG's TXT record that helps prevent spam emails.

Service (SRV) - Designates the IP address and the port number of servers in case it needs to be serviced.

Name server (NS) - This lists the name server that contains the actual DNS information location. This tells devices where to go to find the IP address of an actual domain.

Teacher Notes:

```
┌──(kali@10.1.17.234)-[~]
└─$ nslookup -query=NS cyber.org
Server:         10.3.0.2
Address:        10.3.0.2#53

Non-authoritative answer:
cyber.org       nameserver = ns16.domaincontrol.com.
cyber.org       nameserver = ns15.domaincontrol.com.
```

CYBER.ORG's NS record

Notice that CYBER.ORG's DNS records are located on two different root servers.

How does it work?

How do the DNS servers work with your computer when a web address is entered? The first step is the user typing in the URL of the webpage they want to go to. This creates a query that goes to find the IP address that is associated with that domain name. Typically, the first place the query will check is the DNS cache. ***DNS cache*** is when IP addresses and domain names are saved from previous visits for quicker DNS queries. These DNS caches are typically store on a user's system, on an organization's server, or sometimes on the ISP's (internet service provider) server. The ISP's cache/lists are so big, this is one of the most popular ways a system resolves a DNS query. Searching these lists is known as a ***recursive*** or ***iterative lookup***. It will check a list, if it's not there, then it moves on to the next list and so on. These recursive lists have a ***TTL***, or ***time to live***, setting for the domain, this just meaning that the lists will recheck the domain/IP address every so often, depending on the current TTL setting.

However, if the query is not successful with using the DNS cache or with recursive lookups, the query goes to the root servers, or the ***authoritative name servers***. These servers start at the top-level domain (TLD) servers, this means that it first sorts the URL by the ending. Popular top-level domains are .com, .org, .net, .edu, etc… Then, these TLD servers will send the request to the proper DNS server that contains the domain for that specific top-level. There, the query should be able to find the proper DNS record to match up the domain name with an IP address. This IP address is returned to the original system which sends the request to that IP address.

Teacher Notes:

Other DNS terms

Internal vs. External – Internal DNS is when a company wants to set up their own domains for inside a specific network. External is the normal DNS settings that are the same for all systems on connected to the WAN.

Zone Transfers – This is when a server will download an entire DNS from a DNS server/zone. This is done via the AXFR protocol and allows for backups of the DNS servers and creation of the recursive servers.

Reverse DNS/Reverse Lookup – A query that sends an IP address to find the domain name associated with that IP address.

Forward Lookup – A query that sends the domain name to find the IP address associated with that domain name.