COMPENG 4DN4 Lab 1 Report

Aaron Pinto
pintoa9

Raeed Hassan
hassam41

February 12, 2023

TCP: Wireshark

Figure 1: http://compeng4dn4.mooo.com:50008/photos/351.jpeg

TCP: WinDump

DNS

The `nslookup` utility was used to do a DNS query on the `compeng4dn4.mooo.com` server. The terminal output of the DNS query is shown in Listing 1.

Listing 1: DNS Query Terminal Output

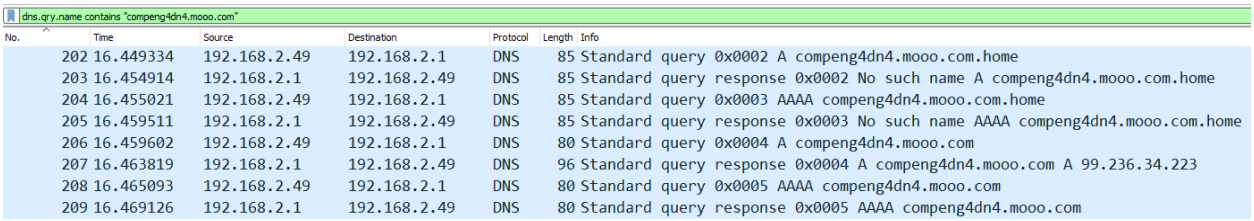
```
nslookup compeng4dn4.mooo.com
Server:  mynetwork
Address:  192.168.2.1

Non-authoritative answer:
Name:    compeng4dn4.mooo.com
Address:  99.236.34.223
```

The Wireshark capture for the DNS query is shown below in Figure 2. The capture was filtered for DNS queries containing `compeng4dn4.mooo.com`, using the display filter `dns.qry.name contains "compeng4dn4.mooo.com"`.

The DNS query first searches for `compeng4dn4.mooo.com` with the DNS suffix `.home`, performing the query with "A" and "AAAA" records, for mapping hostnames to IPv4 and IPv6 addresses. Both DNS queries return "no such name" indicating that the queries are unsuccessful. The DNS query then queries `compeng4dn4.mooo.com` with no suffix, returning the correct IPv4 address for the A record. The AAAA record does not return any address.

Figure 2: DNS Query Display Filter



Traceroute

Nmap