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

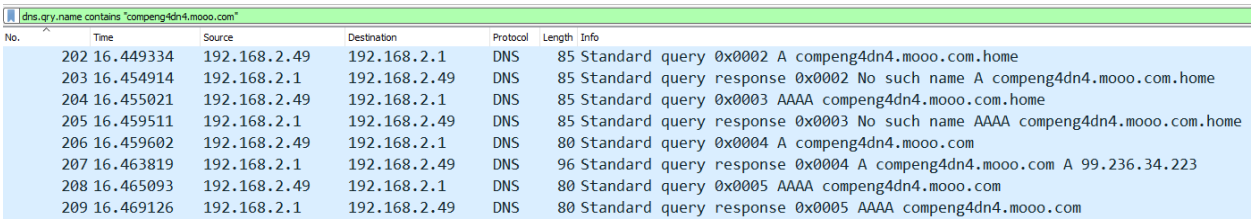
```
nslookup compeng4dn4.mooo.com
Server:  mynetwork
Address:  192.168.2.1

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 WireShark Capture



dns.qry.name contains "compeng4dn4.mooo.com"

No.	Time	Source	Destination	Protocol	Length	Info
202	16.449334	192.168.2.49	192.168.2.1	DNS	85	Standard query 0x0002 A compeng4dn4.mooo.com.home
203	16.454914	192.168.2.1	192.168.2.49	DNS	85	Standard query response 0x0002 No such name A compeng4dn4.mooo.com.home
204	16.455021	192.168.2.49	192.168.2.1	DNS	85	Standard query 0x0003 AAAA compeng4dn4.mooo.com.home
205	16.459511	192.168.2.1	192.168.2.49	DNS	85	Standard query response 0x0003 No such name AAAA compeng4dn4.mooo.com.home
206	16.459602	192.168.2.49	192.168.2.1	DNS	80	Standard query 0x0004 A compeng4dn4.mooo.com
207	16.463819	192.168.2.1	192.168.2.49	DNS	96	Standard query response 0x0004 A compeng4dn4.mooo.com A 99.236.34.223
208	16.465093	192.168.2.49	192.168.2.1	DNS	80	Standard query 0x0005 AAAA compeng4dn4.mooo.com
209	16.469126	192.168.2.1	192.168.2.49	DNS	80	Standard query response 0x0005 AAAA compeng4dn4.mooo.com

Traceroute

The traceroute terminal output is shown below in Listing 2. We can see that the traceroute begins first with a hoop to the local router at 192.168.2.1, then takes 10 hops to route to 24.156.158.102, with all subsequent hops timing out.

Listing 2: Traceroute Terminal Output

```
tracert compeng4dn4.mooo.com

Tracing route to compeng4dn4.mooo.com [99.236.34.223]
over a maximum of 30 hops:

  1     5 ms     5 ms     5 ms  mynetwork [192.168.2.1]
  2    22 ms    15 ms    19 ms  10.11.2.49
  3     *        *        *     Request timed out.
  4    14 ms    21 ms     *     cksnon1673w_lag37.net.bell.ca [142.124.127.44]
  5     9 ms    18 ms    22 ms  cr01-toroonxnhe9-bundle-ether1.net.bell.ca [142.124.127.159]
  6    22 ms    26 ms    24 ms  bx5-torontoxn_ae0.net.bell.ca [64.230.52.229]
  7    29 ms    28 ms    20 ms  rogers_bx5-torontoxn.net.bell.ca [184.150.158.205]
  8    22 ms    20 ms    21 ms  209.148.235.221
  9    23 ms    13 ms    15 ms  3039-dgw01.hstr.rmgt.net.rogers.com [209.148.237.94]
  10    23 ms    33 ms    18 ms  24.156.158.102
  11     *        *        *     Request timed out.
  12     *        *        *     Request timed out.
  13     *        *        *     Request timed out.
  14     *        *        *     Request timed out.
  15     *        *        *     Request timed out.
  16     *        *        *     Request timed out.
  17     *        *        *     Request timed out.
  18     *        *        *     Request timed out.
  19     *        *        *     Request timed out.
  20     *        *        *     Request timed out.
  21     *        *        *     Request timed out.
  22     *        *        *     Request timed out.
  23     *        *        *     Request timed out.
  24     *        *        *     Request timed out.
  25     *        *        *     Request timed out.
  26     *        *        *     Request timed out.
  27     *        *        *     Request timed out.
  28     *        *        *     Request timed out.
  29     *        *        *     Request timed out.
  30     *        *        *     Request timed out.
```

```
Trace complete.
```

The WireShark capture was done with a capture filter of `icmp`. The WireShark capture for traceroute is shown below in Figure 3. We can see that what the traceroute command does is continually send ICMP echo requests to the targeted hostname (99.236.34.223) from 192.168.2.49 (the `localhost`). We can also follow the hops in the traceroute by checking the source destination of the "Time-to-live exceeded" ICMP packets, with the first two hops of the traceroute (192.168.2.1 and 10.11.2.49) appearing in the figure.

Figure 3: Traceroute WireShark Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=236/60416, ttl=1 (no response found!)
2	0.000016	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=236/60416, ttl=1 (no response found!)
3	0.005391	192.168.2.1	192.168.2.49	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
4	0.006001	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=237/60672, ttl=1 (no response found!)
5	0.006013	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=237/60672, ttl=1 (no response found!)
6	0.011327	192.168.2.1	192.168.2.49	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
7	0.011721	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=238/60928, ttl=1 (no response found!)
8	0.011727	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=238/60928, ttl=1 (no response found!)
9	0.017607	192.168.2.1	192.168.2.49	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
10	1.022108	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=239/61184, ttl=2 (no response found!)
11	1.022119	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=239/61184, ttl=2 (no response found!)
12	1.044148	10.11.2.49	192.168.2.49	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
13	1.044623	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=240/61440, ttl=2 (no response found!)
14	1.044629	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=240/61440, ttl=2 (no response found!)
15	1.060458	10.11.2.49	192.168.2.49	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
16	1.061046	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=241/61696, ttl=2 (no response found!)
17	1.061062	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=241/61696, ttl=2 (no response found!)
18	1.080493	10.11.2.49	192.168.2.49	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
19	7.026845	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=242/61952, ttl=3 (no response found!)
20	7.026854	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=242/61952, ttl=3 (no response found!)
21	10.974409	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=243/62208, ttl=3 (no response found!)
22	10.974426	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=243/62208, ttl=3 (no response found!)
23	14.969557	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=244/62464, ttl=3 (no response found!)
24	14.969568	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=244/62464, ttl=3 (no response found!)
25	18.972363	192.168.2.49	99.236.34.223	ICMP	106	Echo (ping) request id=0x0001, seq=245/62720, ttl=4 (no response found!)

Nmap