Application Layer (DNS) — Lab 2 part 2

A. Murad, D. Palma

Contents

Introduction

The goal of this lab is to learn how to setup and configure your own DNS server as well as capturing and analyzing DNS packets. The lab has several **milestones**. Make sure you reach each one before advancing to the next.

For delivery, submit a PDF report where you answer **only** those steps that are marked with **REPORT(%)**. Additionally, you should submit the codes or capture files, if they were **explicitly** asked for. The percent point gives you an indication of the score of that question. Lab2 (both parts) counts for **4 points** of your final score in this course.

System Setup

We will use the system setup as in part1, but we will build the DNS server for the "ttm4200_net", as shown in figure 1.

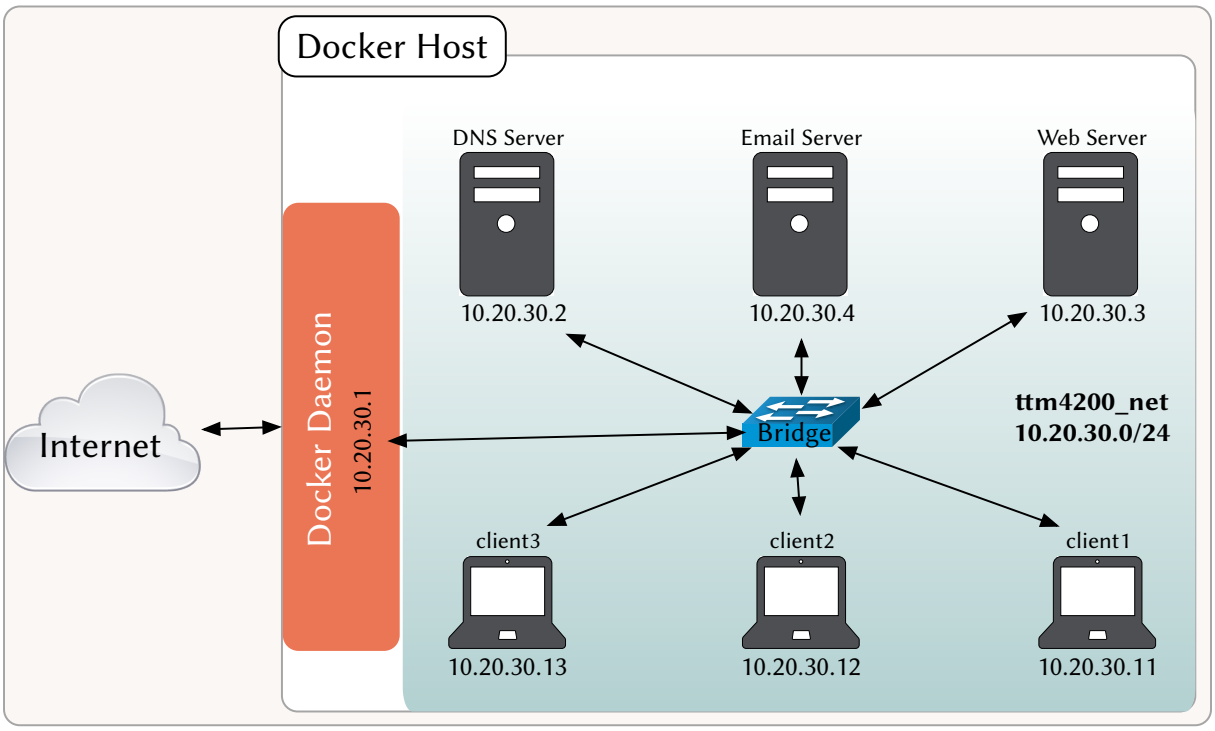

Figure 1: System Setup

- Build the images and start the container using the attached docker-compose file.

1 Milestone 1 –Set up a DNS Server

In this lab, you will set up and run your own authoritative name server. We will use BIND9 (https://www.isc.org/bind/) which is an open source DNS system.

1.1 Configure *BIND9*

BIND9 is already installed in the "dnsserver" image but you need to configure it as the **authoritative** name server for the domain "ttm4200.com". The configuration files are stored in "/etc/bind/".

- Configure *BIND9* options (in "named.conf.options") to:
  - allow queries only from your private network
  - forward unknown queries to other DNS servers (e.g. NTNU's DNS server: "129.241.0.200")
  - enable recursive queries.
  - You can start with this template by filling it with your own configurations:

```
options {
      # a directory  where BIND) stores its cache (previously resolved domain names)
         directory "/var/cache/bind";

         listen-on port ==== fill in here ==== { ==== fill in here ==== };

         allow-query { ==== fill in here ==== };

         forwarders { ==== fill in here ====  };

         recursion ==== fill in here ====;
      };
```

1.2 DNS Forward Lookup

The forward lookup zone (https://en.wikipedia.org/wiki/Zone_file) stores DNS Record (hostname to IP address relations) for your domain.

- Create a forward lookup for "ttm4200_net" network, as shown in figure 1. Call the zone file "ttm4200.com.zone" and place in "/etc/bind/". You can start by filling out this template (note that the semicolon is a comment in zone files):

```
;Defines base name -used in domain name substitution
; @ symbol is replaced with the current value of $ORIGIN.
$ORIGIN ttm4200.com.

;Time to Live value for the zone
$TTL 1h
```

```
;A Start of Authority record that contain administrative information about the zone
;especially regarding zone transfers.
@               IN  SOA   ns.ttm4200.com. root.ttm4200.com. (
                        2019111001; serial
                        1d ; refresh
                        2h ; retry
                        4w ; expire
                        1h ); minimum

;Address record for the webserver ttm4200.com.
@              IN  A     10.20.30.3
               IN  AAAA  fd00::3

;Alias records (CNAME) for www.ttm4200.com
==== fill in here ====

;Name Server record (NS) for ttm4200.com. that define which servers serve copies of
;this zone (it must point to an A record and/or AAAA record)
==== fill in here ====

;Mail Exchange record (MX) for ttm4200.com. that define where email should be sent
;to and at what priority (it must point to an A record and/or AAAA record)
==== fill in here ====
```

- Add your forward zone to *BIND9*, thus turning it into a Primary Master server for your domain. You can edit the file "/etc/bind/named.conf.local" to do that.

```
# your domain name
zone ==== fill in here ==== IN {
        type master;
        # file name of your forward zone (full path)
        file ==== fill in here ====;
};
```

- Check you configuration syntax with the command `named-checkconf` and your zone file syntax (`named-checkconf -z`).
- Restart *BIND9* (`sudo service bind9 restart`).

2 Milestone 2 – Analyzing DNS Packets

- Start a packet capturing with `tcpdump` on your DNS server and dump it to a file (e.g. "dns_capture.pcap").
- In a client container (e.g. client2), configure it to use your DNS server as its nameserver (in "/etc/resolve.conf"):

```
nameserver ==== fill in here ====
```

- In your client container, run the following queries:
  - Run `nslookup` to obtain the IP address of `ttm4200.com`
  - Run `nslookup` to determine the authoritative DNS server of `ttm4200.com`
  - Run `nslookup` to determine the mail server for `ttm4200.com`
  - Run `dig` to query for any-type of record information in the domain `ttm4200.com`

Q1. **REPORT(4%):** Provide a screenshot of the previous queries and shortly explain the results.

- Copy the packet trace file (e.g. "dns_capture.pcap") to your host machine and open it with `wireshark`.
- Show only the DNS based traffic (write "dns" in the display filter). Look at the last query and response messages, then answer the following questions and validate your answer with an **annotated** screenshot from Wireshark:

  Q2. **REPORT(2%):** What is the destination port for the DNS query message? What is the source port of the DNS response message?

  Q3. **REPORT(2%):** To what IP address is the DNS query message sent?

  Q4. **REPORT(3%):** Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

  Q5. **REPORT(3%):** Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

Q6. **REPORT(4%):** Submit your capture file "dns_capture.pcap" along with the report.

3 Milestone 3 – DNS Reverse Lookup

Reverse lookup zones are used to resolve IP addresses to host names, rather than host names to IP addresses. For more information on how to create a reverse zone you can read this guide (https://www.apnic.net/about-apnic/corporate-documents/documents/resource-guidelines/reverse-zones/).

- Create a reverse lookup zone for your private network. Call it "rev-ttm4200.com.zone" and place it in "/etc/bind". You can start by filling out this template:

```
;reverse domain name
$ORIGIN 30.20.10.in-addr.arpa.
$TTL 1h
; Start of Authority (SOA) record
@          IN  SOA   ns.ttm4200.com. root.ttm4200.com. (
                                    2019111001; serial
                                    1d ; refresh
```

```
                                        2h ; retry
                                        4w ; expire
                                        1h ); minimum
;Nameserver (NS) records declaring the nameserver that serve this zone
@         IN  NS    ns.ttm4200.com.

;pointer (PTR) records for each IP address
;PTR for ns ns.ttm4200.com.
==== fill in here ====

;PTR for ns mail.ttm4200.com.
==== fill in here ====

;PTR for ns www.ttm4200.com.
==== fill in here ====
```

- Add your reverse zone to *BIND9*. You can fill in the example below and add it to "named.conf.local".

```
# reverse domain name
zone ==== fill in here ==== IN {
        type master;
        # file name of your forward zone (full path)
        file ==== fill in here ====;
};
```

- Restart *BIND9*, then check you configuration and zone file syntax.

4 Milestone 4 - Analyzing Reverse DNS Packets

- Start a packet capture with `tcpdump` on your DNS server and dump it to a file (e.g. "reverse_dns_capture.pcap").
- In your client container, perform a reverse DNS lookup of your mail server IP address (e.g. `dig -x <ip_address>`). Afterwards, stop the packet capture on the DNS sever.

Q7. **REPORT(3%):** Provide a screenshot of the previous query and shortly explain the results.

- Copy the packet trace file (e.g. "reverse_dns_capture.pcap") to your host machine and open it with `wireshark`.
- Show only the DNS based traffic. Look at the last query and the response message, then answer the following questions and validate your answer with an **annotated** screenshot from Wireshark:

  Q8. **REPORT(4%):** Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

  Q9. **REPORT(4%):** examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

Q10. **REPORT(4%):** Submit your capture file “reverse_dns_capture.pcap” along with the report.

5 Optional Exercise

Q11. **Extra Credit:** Connect the configured DNS with the Web and Email servers. Capture the traffic from opening a webpage and show the DNS resolution process (include the pcap file).