Internet Security - Lab 4 Report

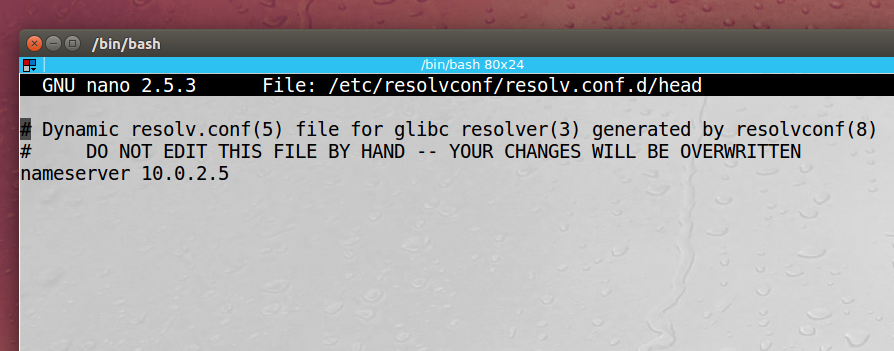
User: 10.0.2.6 (red)

DNS Server: 10.0.2.5 (green)

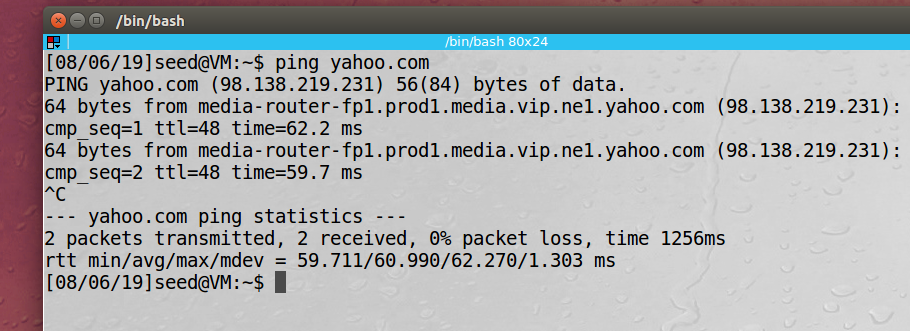
Attacker: 10.0.2.4 (blue)

# Configure the User’s Machine

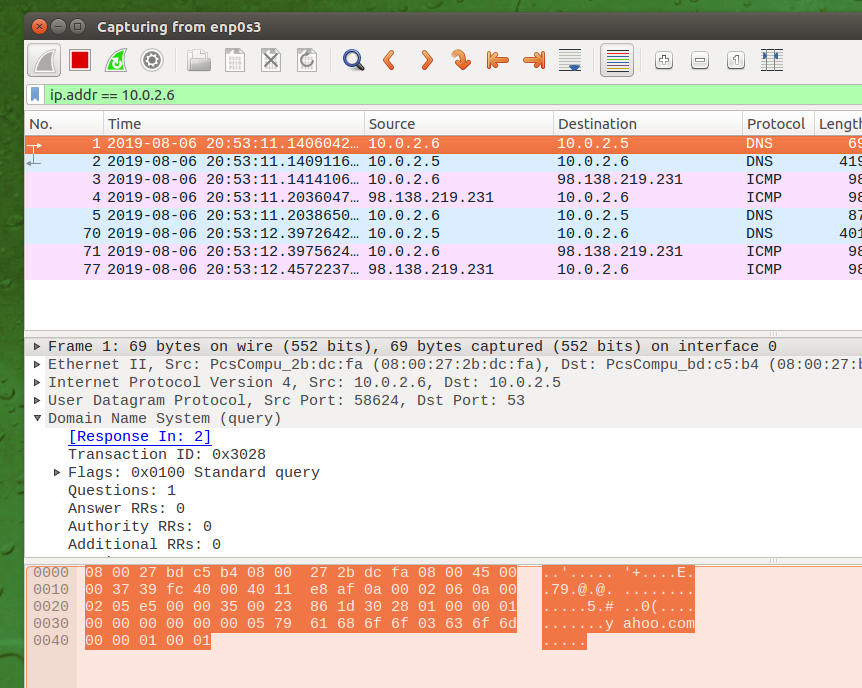
On the user machine we edit the file at /etc/resolvconf/resolv.conf.d/head to change the DNS server to 10.0.2.5:



Then, after refreshing our DNS settings with sudo resolvconf -u, we ping yahoo.com and check that we can resolve the IP and reach the site:



We can see on Wireshark that our user’s DNS is being routed to our local DNS server:

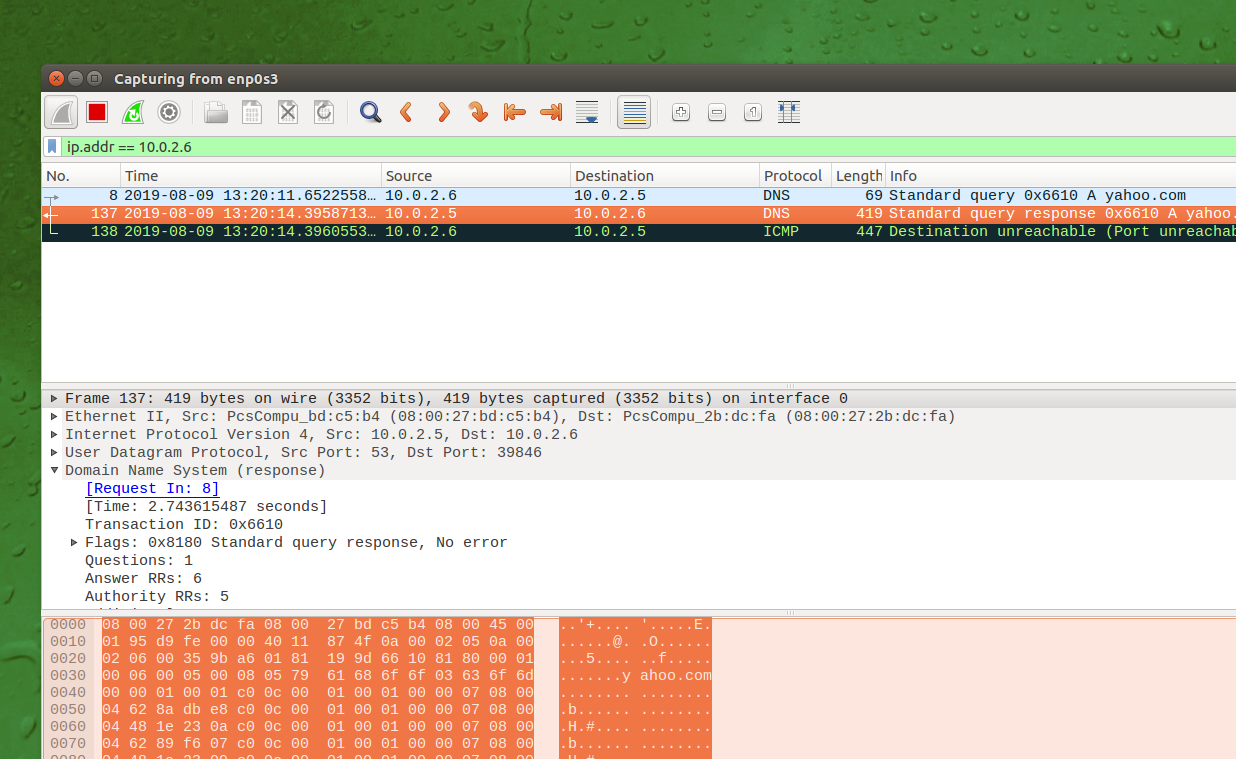


**Observation:** In this task we set up one of our local VMs to act as a DNS server. On our user’s machine we edited the file /etc/resolvconf/resolv.conf.d/head and added the line to redirect our nameserver. We then refreshed DNS settings and tested the server by sending an ICMP echo request to yahoo.com. Then we observed Wireshark and saw a DNS query from our user to the local DNS server.

**Explanation:** Changing the DNS server in Linux can be done very easily, this will allow us to run attacks on the our local VM and its DNS server.

# Setup Local DNS Server

Image of user using our Machine B (10.0.2.5) as the DNS server when we ping yahoo.com:

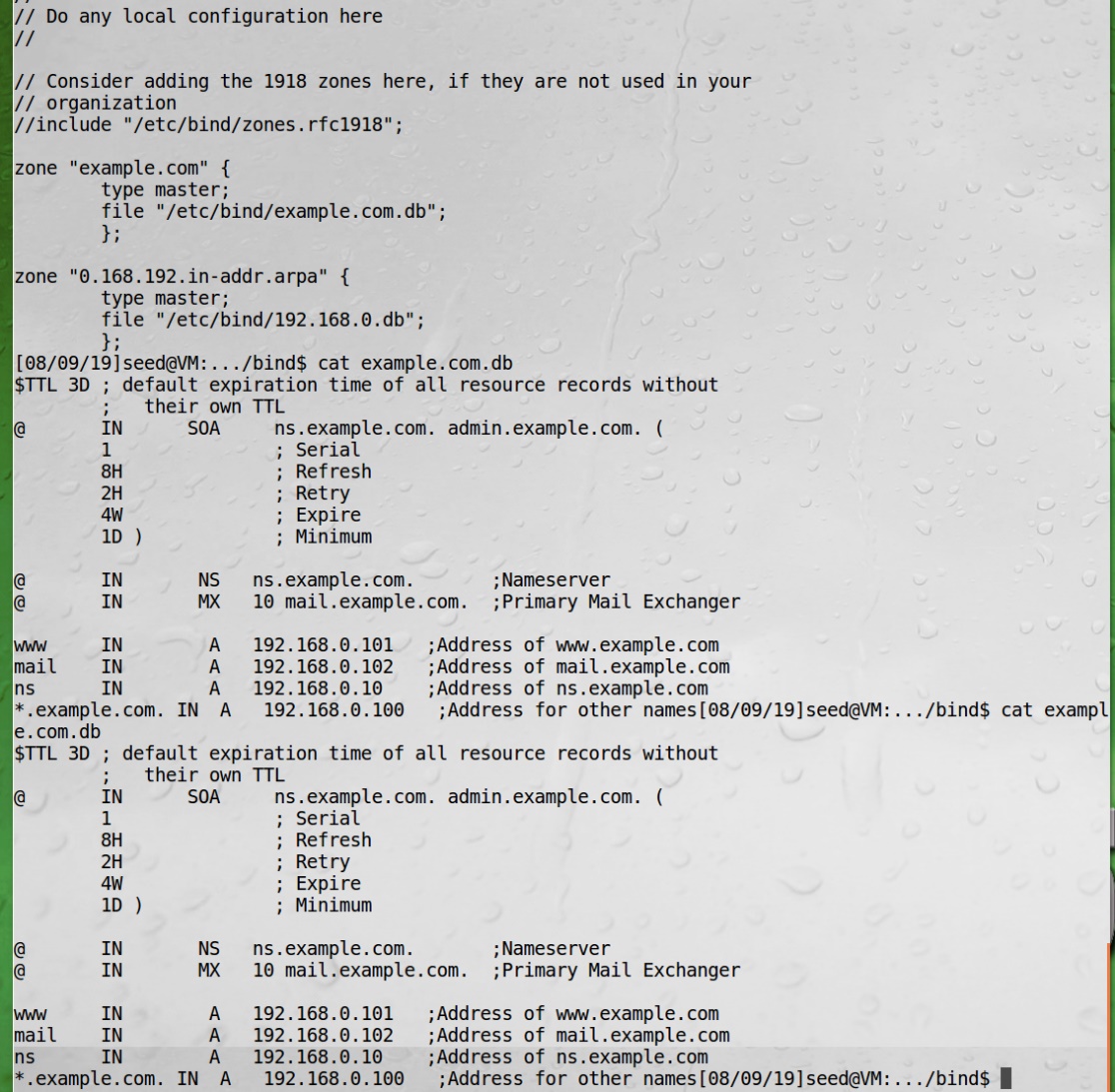


**Observation:** This task had us set up the DNS server on our Ubuntu VM. It showed us how to configure the DNS server options such as DNSSEC and dump files. On my machine I didn’t have to make any changes and the DNS server program “bind9” was already running. Like the previous step we ping yahoo.com from the user machine can capute the packet with Wireshark and verify that we are using the VM as the DNS server.

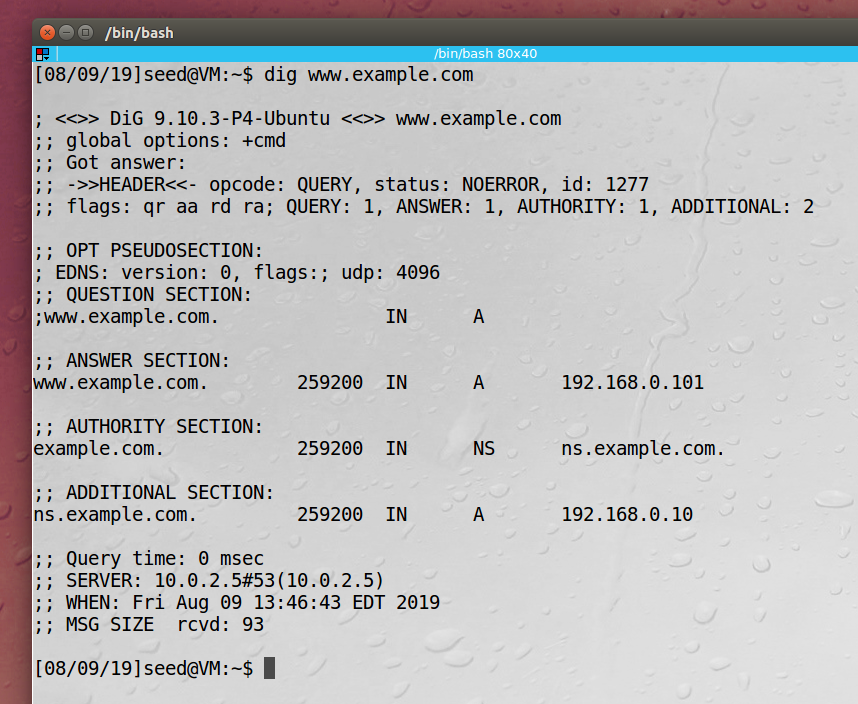
**Explanation:** Changing the DNS server in Linux can be done very easily, this will allow us to run attacks on the our local VM and its DNS server.

# Host a zone in the Local DNS Server

Here we edit three files on our DNS server to update the zones:



Then on the user machine we can dig [www.example.com](http://www.example.com) and see the routing to our local IP:

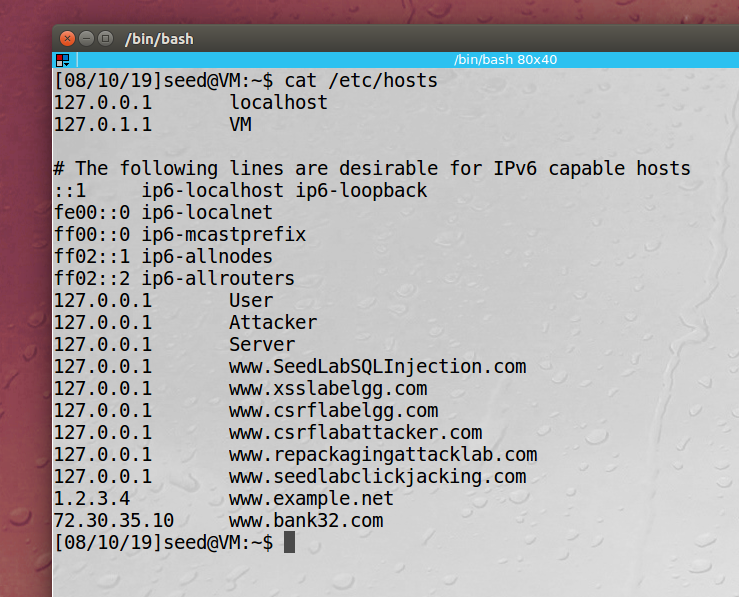


**Observation:** In this task we hosted a zone on our DNS server by creating files for our domain [www.example.com](http://www.example.com). In this file we created DNS records and routing information. We then restart the DNS server, so the changes take effect. Then on our user’s machine we can use the dig command to give us nameserver information about [www.example.com](http://www.example.com) and see that it routes to a local IP address.

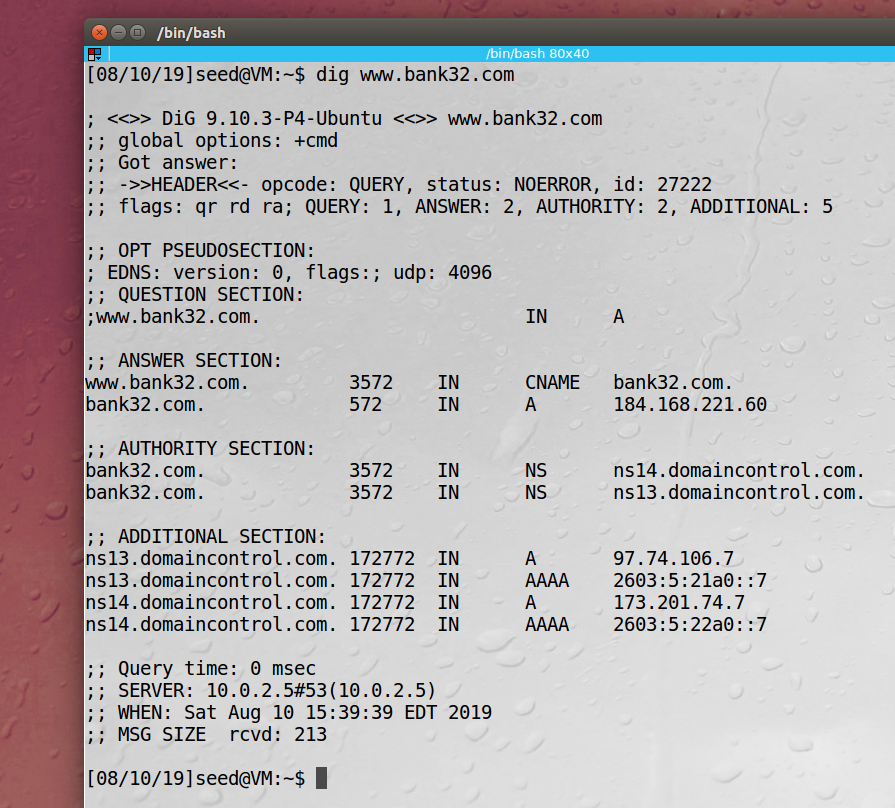
**Explanation:** By editing the bind config file we can direct web addresses to use our local IP address. We can use the dig command to see information about the nameserver or a specific domain.

# Modifying the Host File

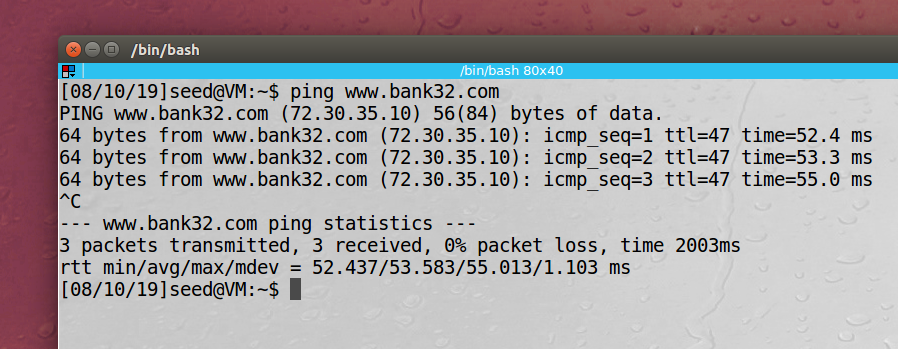
First, we edit the host file on our user’s machine to direct example.net to 1.2.3.4 and [www.bank32.com](http://www.bank32.com) to yahoo.com:



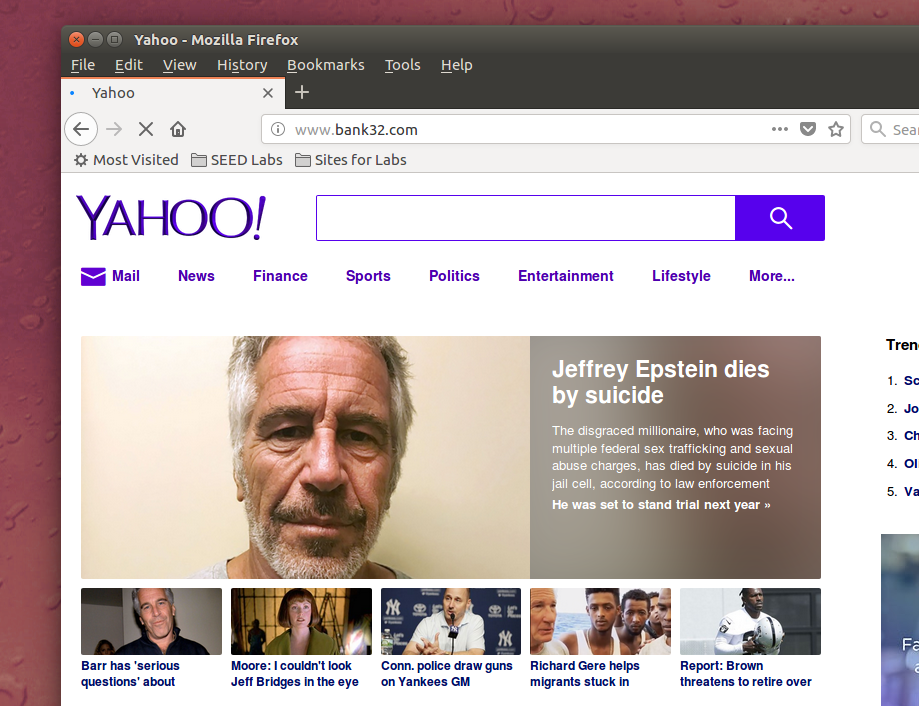
Now we run the dig command to see the IP of bank32.com, dig ignores our host file:



Now we ping [www.bank32.com](http://www.bank32.com) to see where it resolves, ping does not ignore our host file:



Next we open a browser and navigate to [www.bank32.com](http://www.bank32.com) and see that we are redirected to yahoo.com:

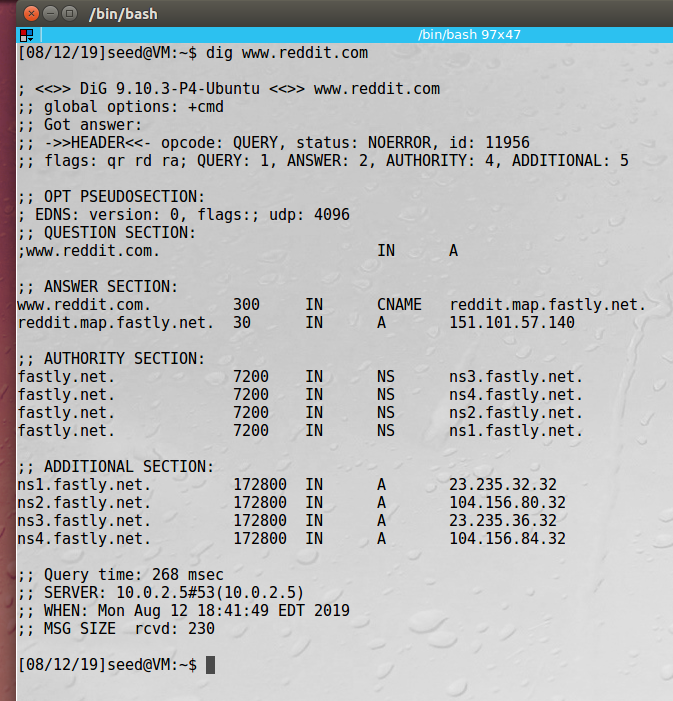


**Observation:** In this task we updated our host file the the User’s machine to redirect [www.example.com](http://www.example.com) to the IP 1.2.3.4 and [www.bank32.com](http://www.bank32.com) to the IP for yahoo.com 72.30.35.10. We then did a dig command to see nameserver information for bank32.com and it didn’t resolve to our new host entry because dig ignores the host file. Next we up we ping bank32.com and see that it resolves to our host file IP entry. Next to show the redirect we open a browser and go to bank32.com and the yahoo site shows up.

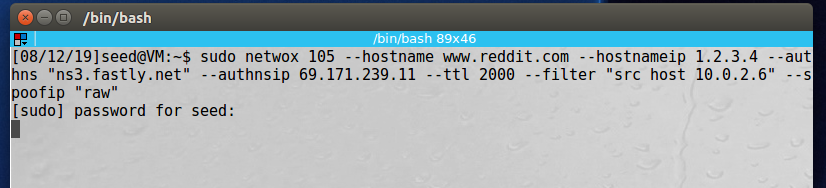
**Explanation:** By editing the host file we can override the DNS server and redirect domains. The dig command ignores these redirects, but ping does not.

# Directly Spoofing Response to User

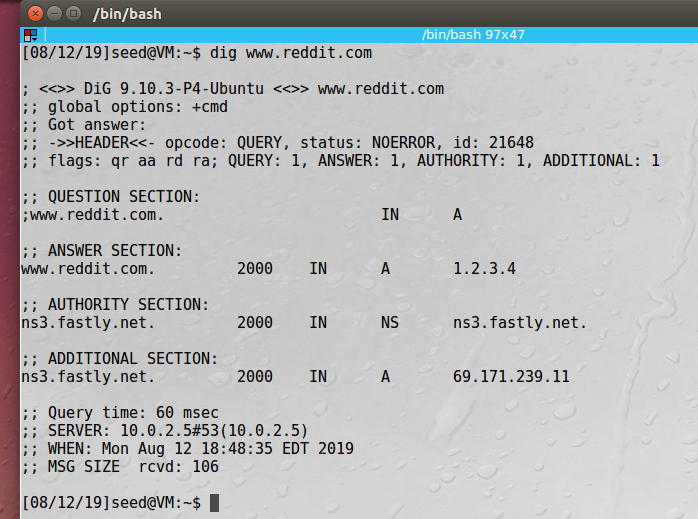
First on the user’s Machine we dig [www.reddit.com](http://www.reddit.com) and resolve the IP Address and the Authority:



Next we clear the cache on our server and on our user machines. And then on the Attacking computer we run the netwox 105 program to spoof the IP Address resolution for [www.reddit.com](http://www.reddit.com) to 1.2.3.4.



Again, on our client machine we run the dig command for [www.reddit.com](http://www.reddit.com), now we see the IP address 1.2.3.4.



And we see on our attacker machine that the DNS attack was successful:

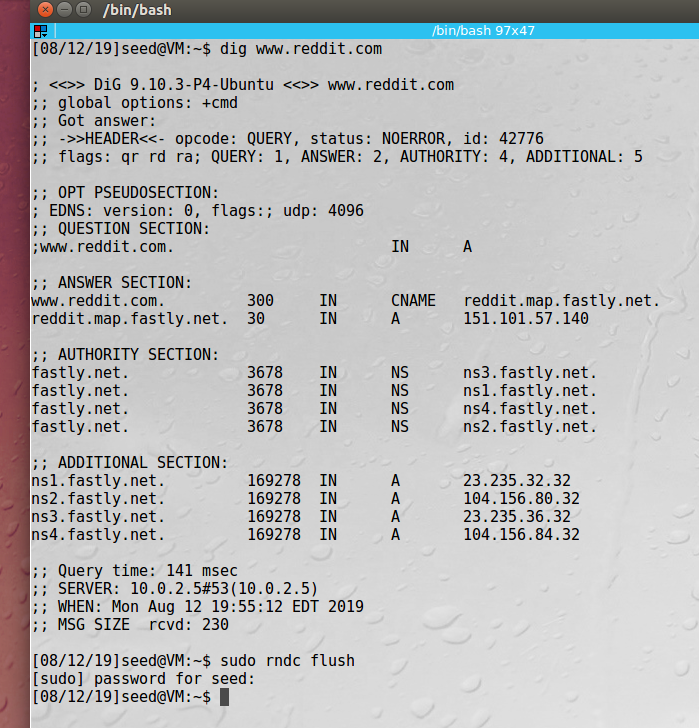


**Observation:** In this task we used the Netwox 105 program to sniff and spoof a DNS query response. We first used the dig command on the user’s machine to resolve [www.reddit.com](http://www.reddit.com) we flushed the DNS cache on the user and our DNS server machines. Next, we ran the Netwox program on the attacker machine, our goal was to return 1.2.3.4 to the user as the IP address of [www.reddit.com](http://www.reddit.com). Finally, on the user machine we execute another dig command and see that it now resolves to 1.2.3.4.

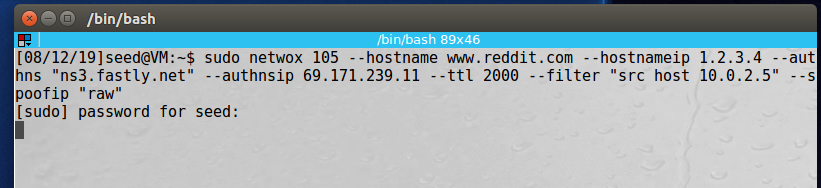
**Explanation:** By using sniffing and spoofing, we can manipulate the DNS and redirect DNS queries. In this attack we were able to make the user think a popular website was at a different IP address.

# DNS Cache Poisoning Attack

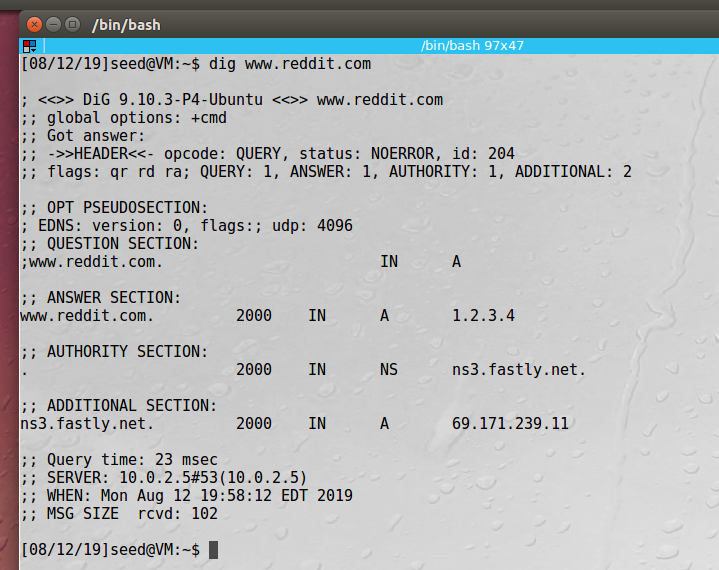
The first thing we do is run a dig command to [www.reddit.com](http://www.reddit.com) on our user’s machine to see where the DNS server resolves:



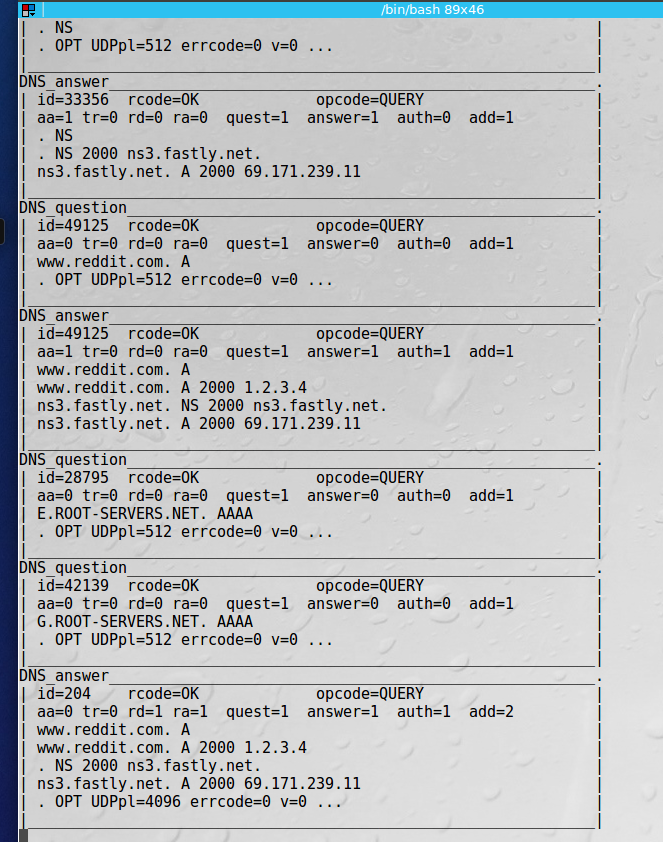
Then we clear cache on our user and DNS server’s machines. Next on our attacker machine we run the Netwox 105 tool to poison the DNS server:



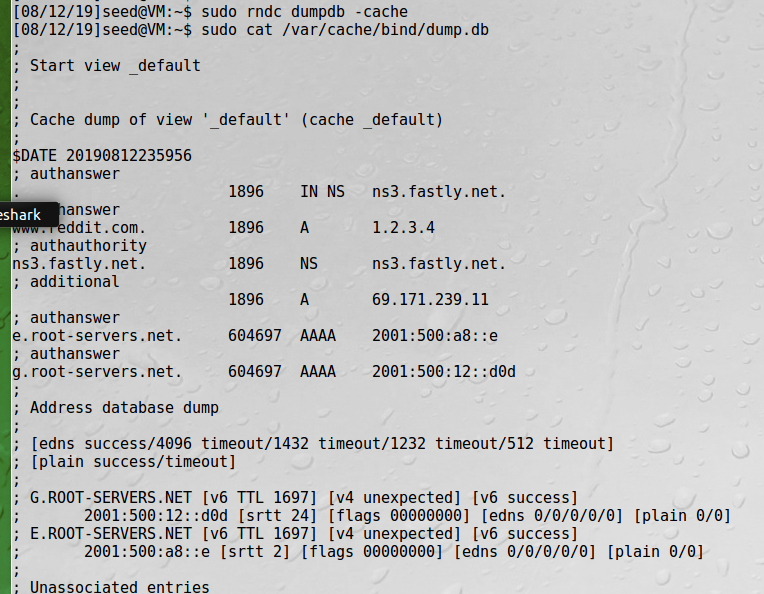
We then run dig on our client machine and see that [www.reddit.com](http://www.reddit.com) resolves to 1.2.3.4:



We can also see the query on out attacker’s machine:



Looking at the dump file on our DNS server machine, we can see that [www.reddit.com](http://www.reddit.com) points to 1.2.3.4:



**Observation:** In this task we used the Netwox 105 program to sniff and spoof a DNS server query. This is like the previous task except this time we are poisoning the DNS Server, not just one user’s query. We first used the dig command on the user’s machine to resolve [www.reddit.com](http://www.reddit.com) we flushed the DNS cache on the user and our DNS server machines. Next, we ran the Netwox program on the attacker machine, our goal was to return 1.2.3.4 to the user as the IP address of [www.reddit.com](http://www.reddit.com). Finally, on the user machine we execute another dig command and see that it now resolves to 1.2.3.4. If we had another machine using the same DNS server it would also point [www.redddit.com](http://www.redddit.com) to 1.2.3.4.

**Explanation:** By using sniffing and spoofing, we can manipulate the DNS and redirect DNS queries. In this attack we were able to trick the DNS server in to thinking reddit.com was at 1.2.3.4. All users on this LAN, who are also using out DNS server will think reddit.com is at 1.2.3.4.