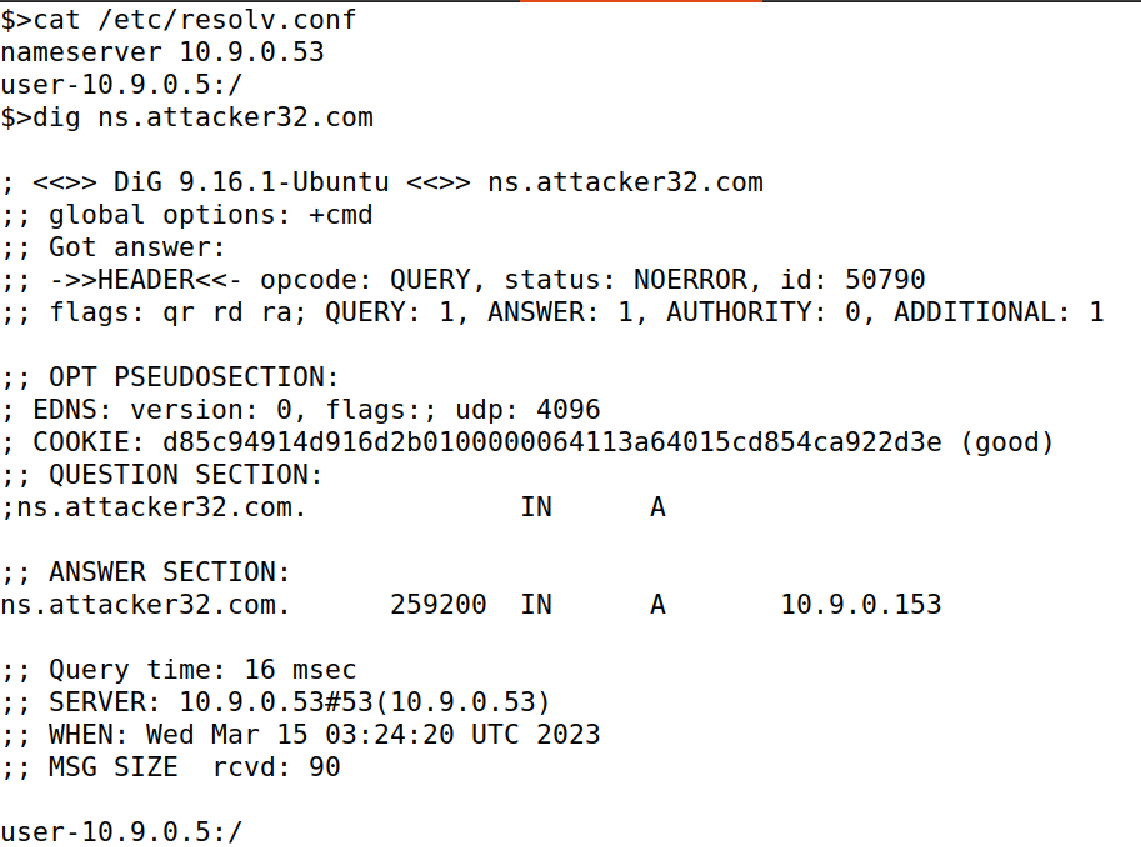
Lab 7:

Task 1: Testing the DNS Setup

Running first dig command in container:



We are getting an answer from attacker container.

Running example domain nameservers dig commands:

Running Official nameserver:

Text

Description automatically generated

We got reply from official server.

Running attacker container:

Text

Description automatically generated

DNS container screenshots:

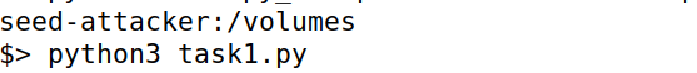
Example.com server entries in DNS container

A picture containing text

Description automatically generated

Task : Directly Spoofing Response to User

Running the python program in attacker container:



Now trying to access a example.com website, for the first time when we ran the dig command, we got the original address now we need to get duplicate address if not our attack failed.

Text

Description automatically generated

Task : DNS Cache Poisoning Attack – Spoofing Answers

Running flush command:

A picture containing shape

Description automatically generated

Running example.com in user container.

Text

Description automatically generated

we can inspect the cache on the local DNS server to see whether it is poisoned or not. The following

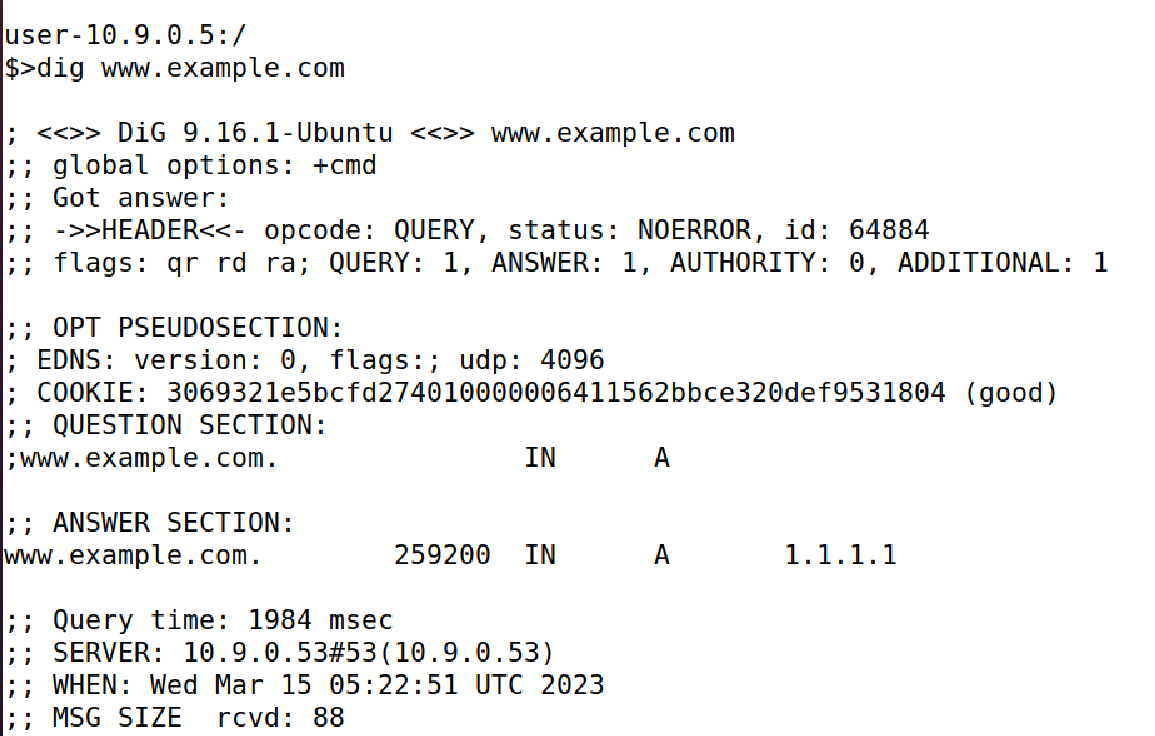
commands first dump the cache into a file, and then display the content of the cache file.

A picture containing graphical user interface

Description automatically generated

Task : Spoofing NS Records

Running dig command in user container:

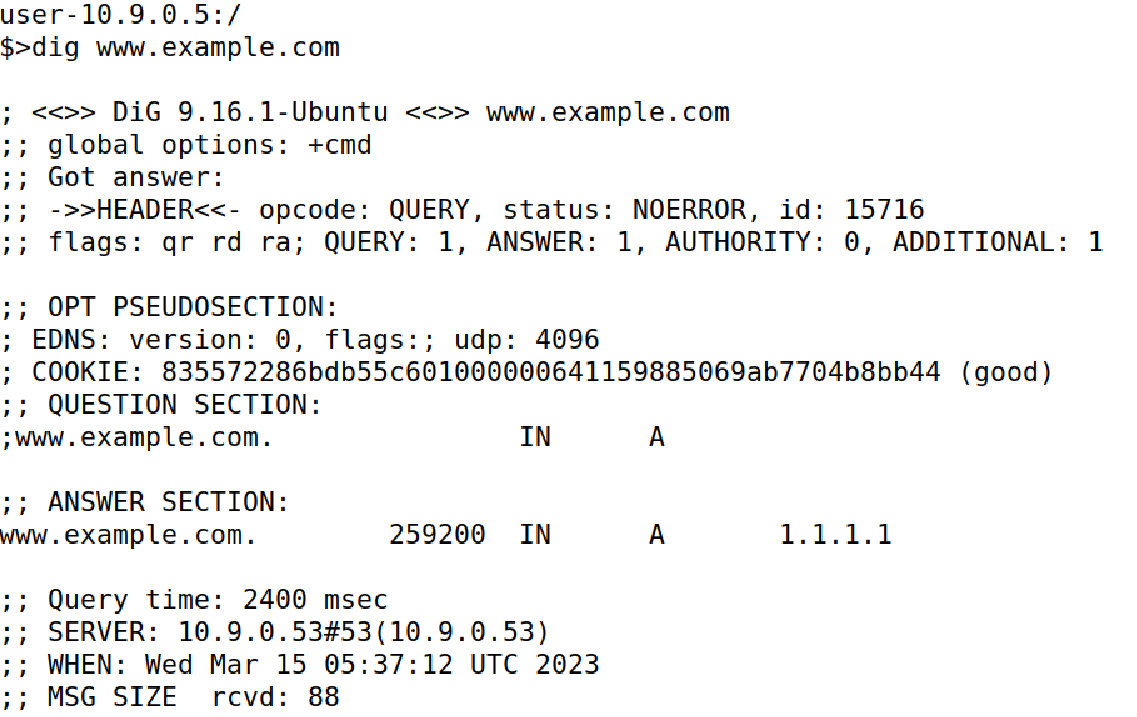


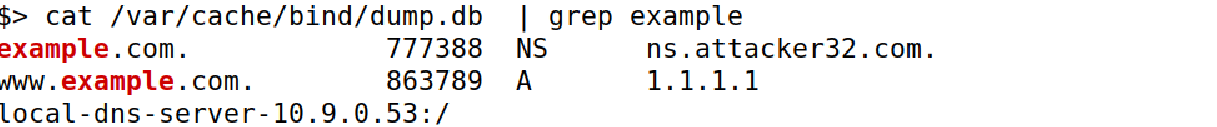
DNS cache:

Graphical user interface, application, Word

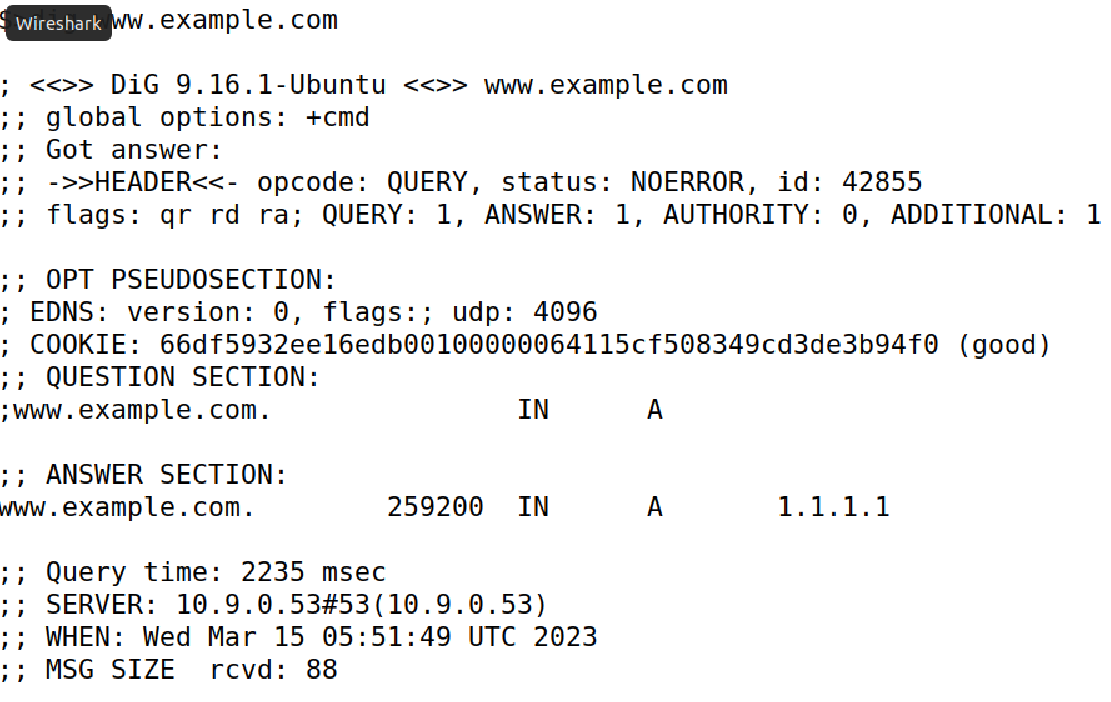
Description automatically generated

Task : Spoofing NS Records for Another Domain





Task : Spoofing Records in the Additional Section



DNS container entry screenshot:

