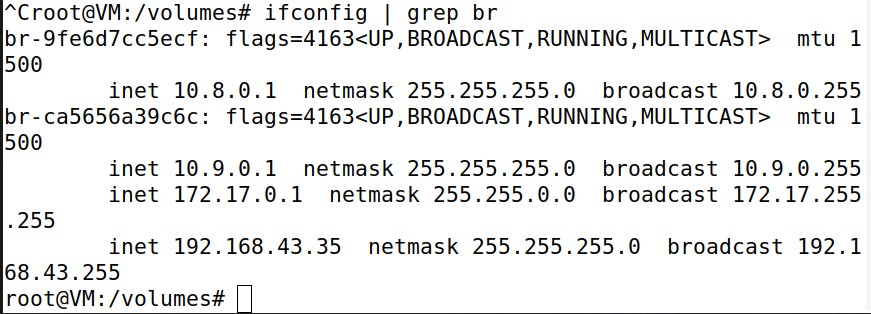
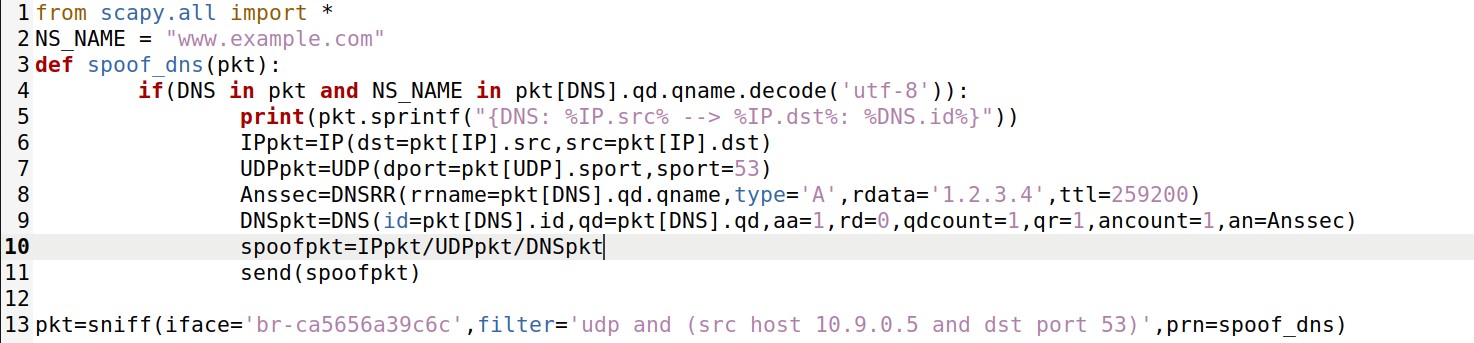
**Local DNS Attack Lab**

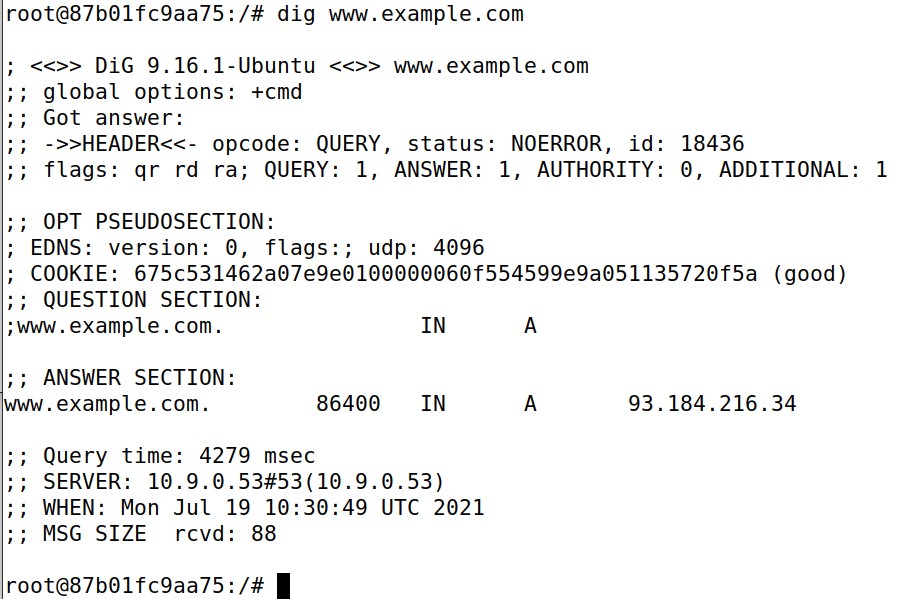
# Task1

实验利用用户会先接受来的较早的报文的原理来进行攻击行为。首先在 router 上增加出网流量延迟，预防欺骗报文来的比合法报文迟的情况。

 查看本机配置情况，用于完成过滤条件等，如下。

 所用攻击代码如下。

 在未运行攻击代码时，在 user 上 dig 某网址，看到 answer 的网址是正常网址 93.184.216.34.

 接着，去 dns 服务器上清空一下缓存，如下。



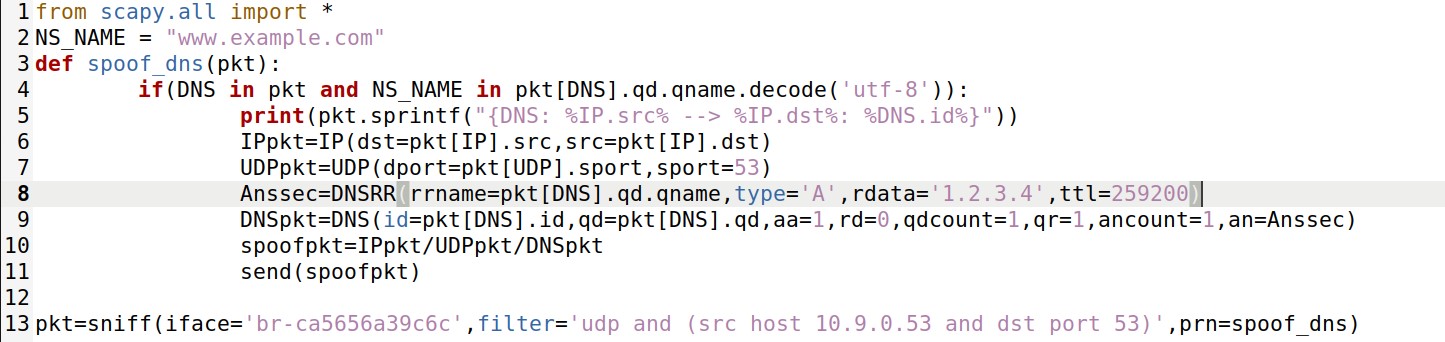
然后，在 attacker 上运行攻击代码，此时终端没有响应，接着到 user 上在 dig 该网址，此时 answer 的网址变成了 1.2.3.4，为伪造的网址。



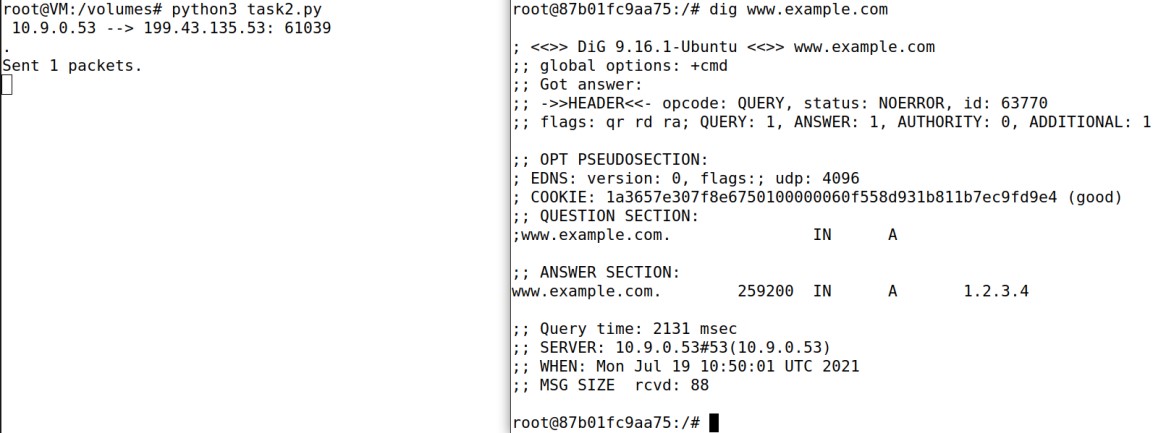
# Task2

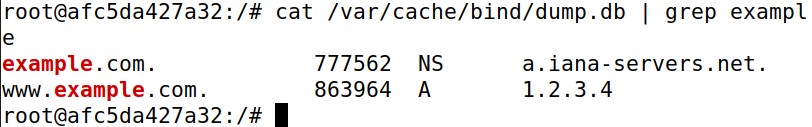
task1 的攻击目标是用户，因此每当用户查询某一网址时，都需要返回一个欺骗报文，为了提高效率，下面将直接攻击 dns 服务器缓存，这样一段时间内，就可以不用不断发送欺骗报文了。

攻击代码如下。

 去 dns 服务器上清空一下缓存。

 运行攻击代码，情况同 Task1.

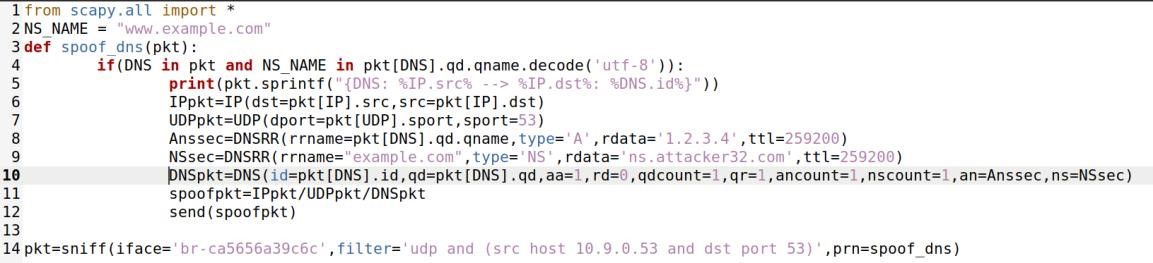
 然后在 dns 服务器上使用 rndc dumpdb -cache 下载缓存，并用如下命令查看，发现缓存已经被修改。

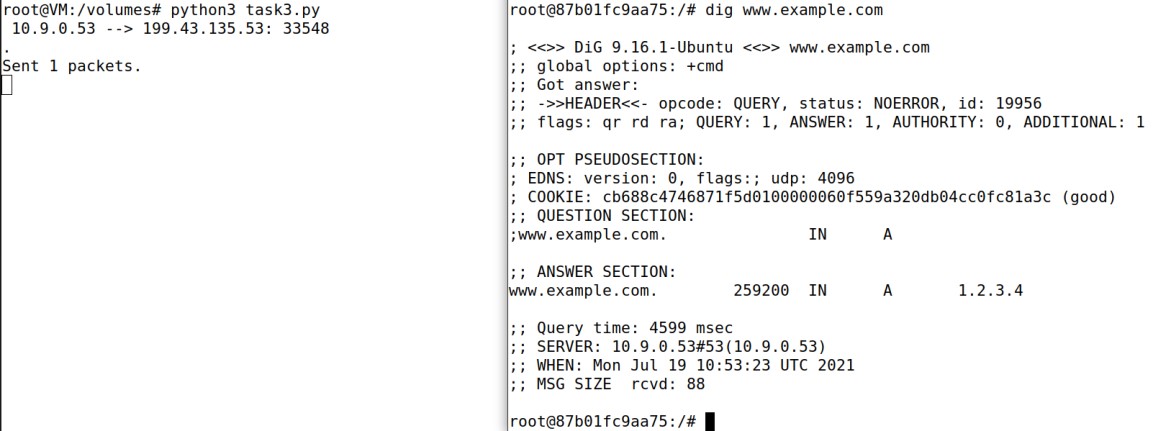


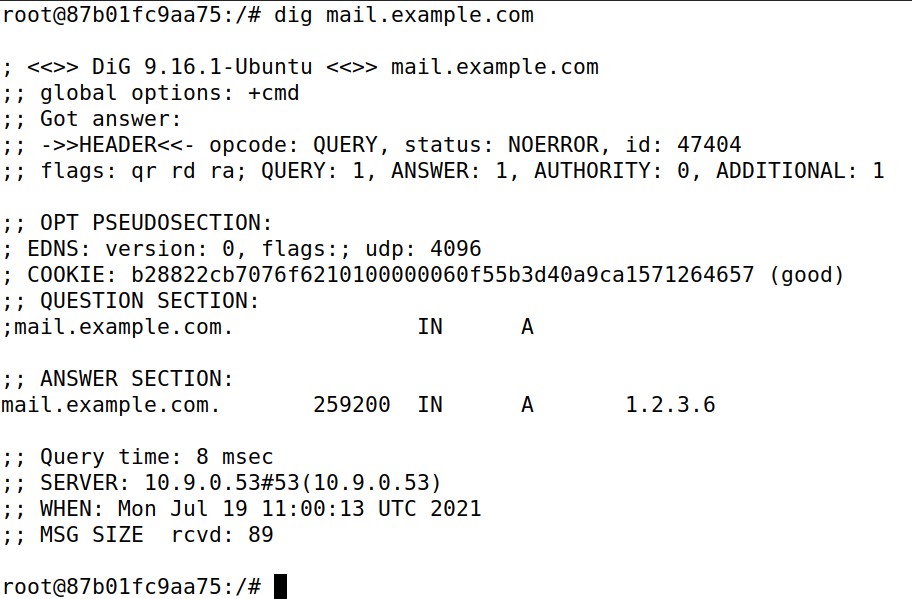
# Task3

上述攻击只影响到 www.example.com 这一个主机名，下面将攻击整个 example.com 内的主机名。

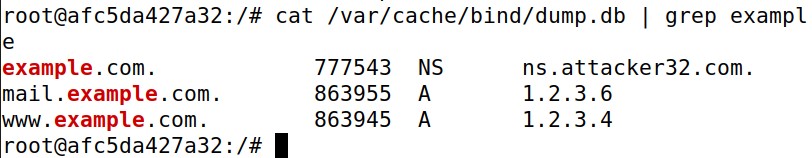
攻击代码如下，新增了 NSsec 这一行。

 清空 dns 服务器缓存，攻击步骤同上。

 这时，在用户上再 dig 一下 example.com 里面的其他主机名，如 mail.example.com，发现 answer 地址也被修改，如下。



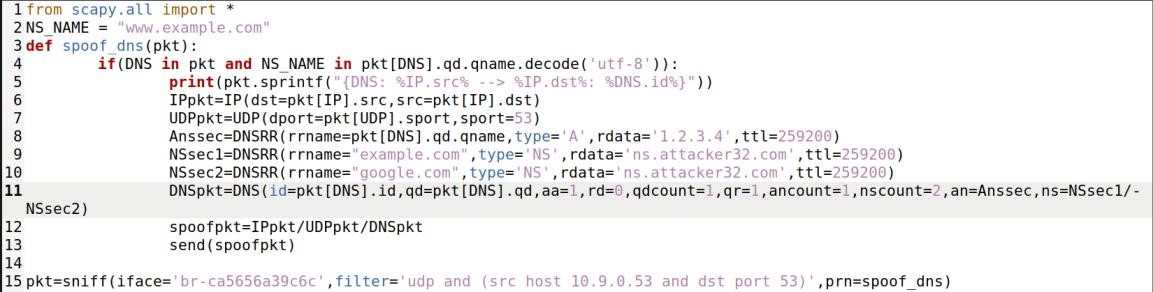
这时查看一下 dns 服务器缓存，发现这两个的地址都被修改了。

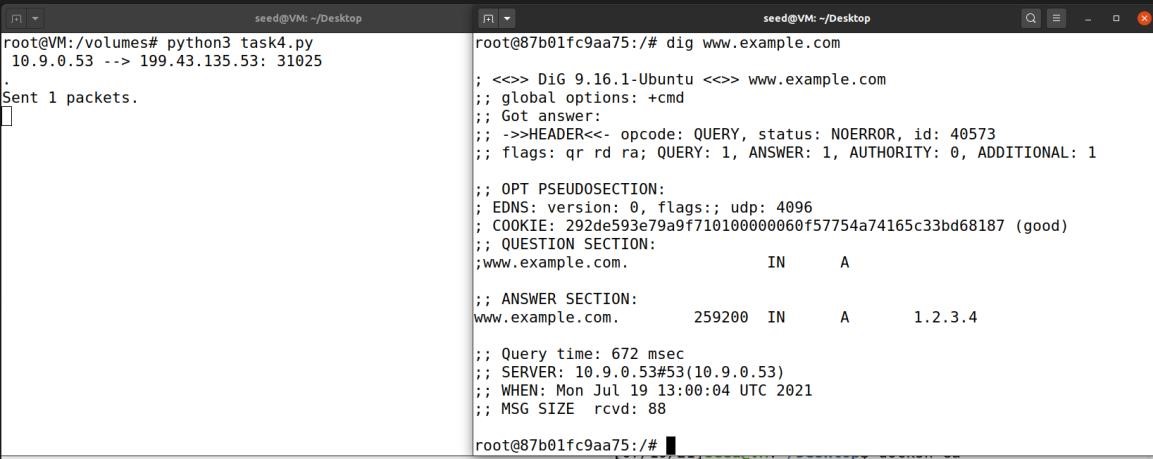


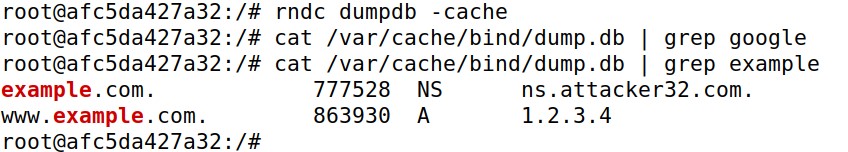
# Task4

上述攻击成功修改了 example.com 的权威域名服务器。下面攻击尝试将该域名服务器用于其他网址。

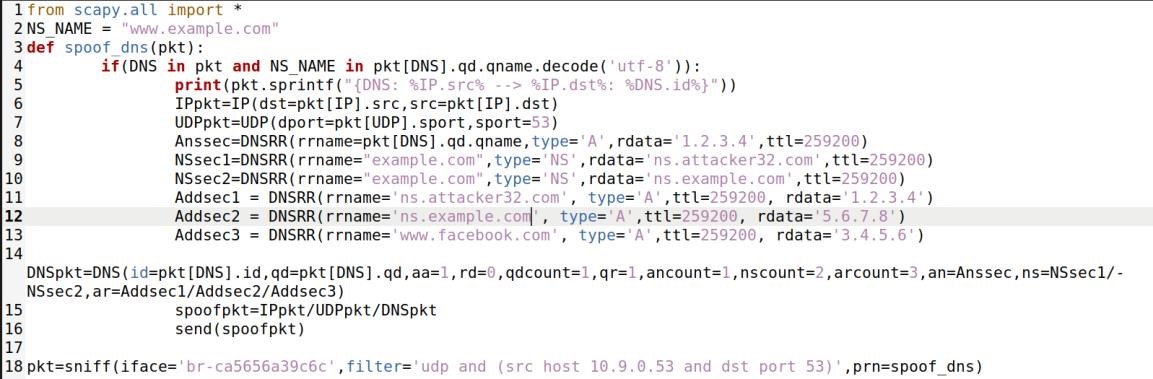
攻击代码如下，修改了 NSsec1，NSsec2 和 DNSpkt 这几行。

 攻击方式同上。

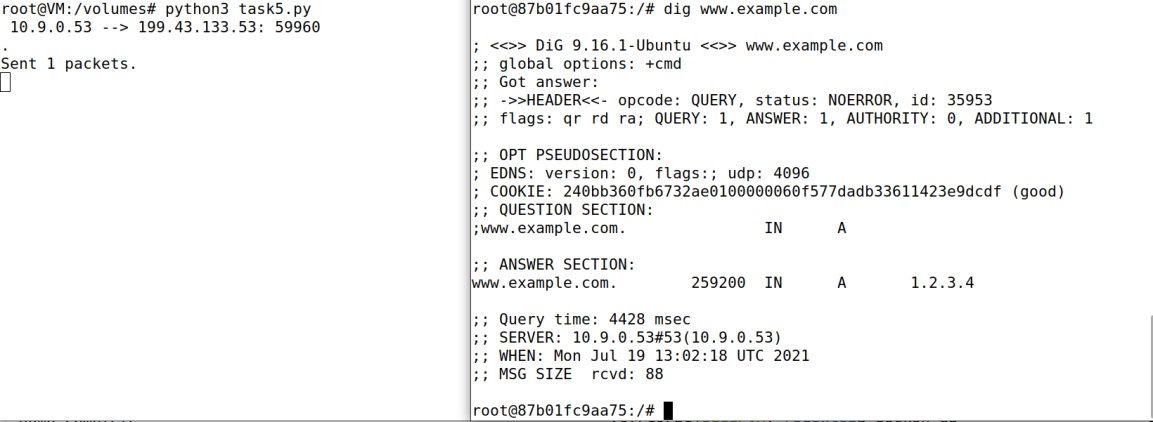
 看一下 dns 服务器的缓存，发现里面并没有 google 的记录。因为如果这条记录被接受了，ns.attacker32.com 就会成为 google.com 的权威域名服务器，而 www.example.com 显然不在 google.com 里面，这显然是不安全的，所以本地 DNS 服务器没有接受。



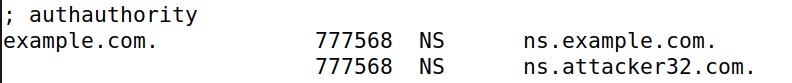
**Task5** 攻击代码如下，修改了 NSsec2，Addsec1，Addsec2，Addsec3 和 DNSpkt 这几行。



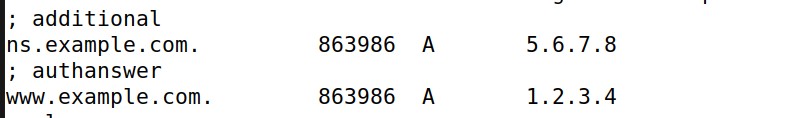
攻击过程同上。



查看 dns 服务器缓存，发现 ns.example.com 和 ns.attacker32.com 都成了 example.com 的权威域名服务器。



ns.example.com 成了附加部分且地址是 5.6.7.8。

 而 facebook 依然找不到。



这时查一下 ns.example.com，但是得到的回复却不是缓存中的 5.6.7.8，因为本地 dns 服务器虽然缓存了这个信息，但是因为安全原因，它并不信任附加部分这些信息，而是重新发送 DNS 请求获得了真正的 IP 地址。

