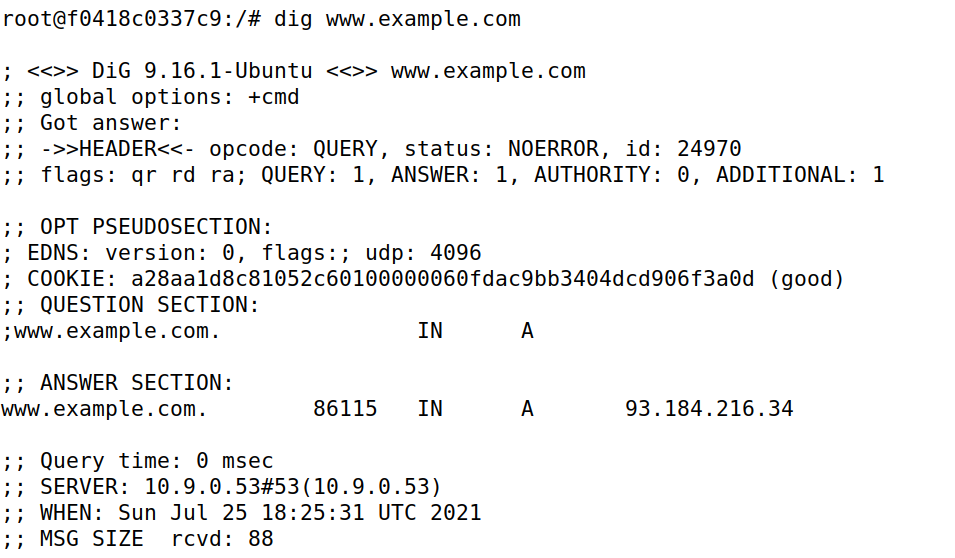
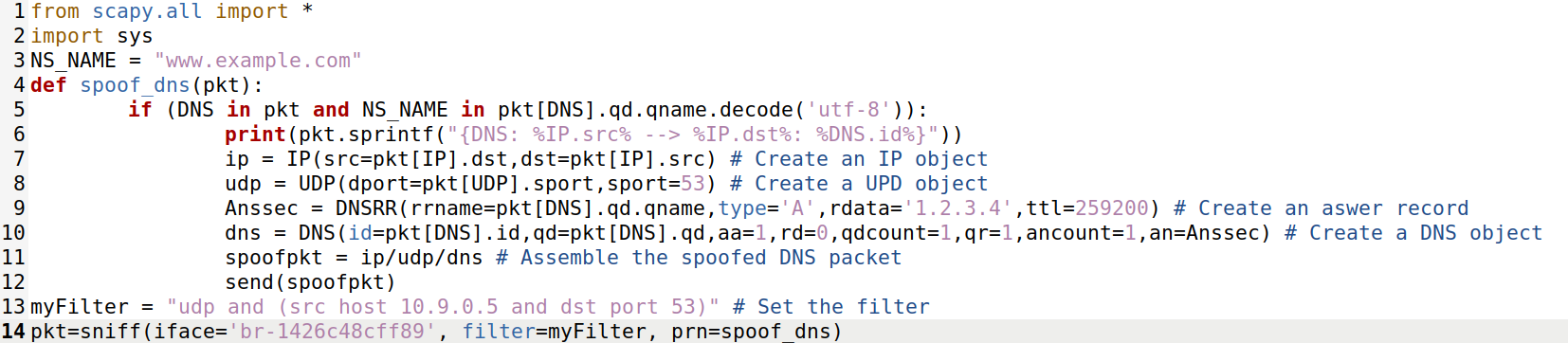
57118127孙博

**Task1**

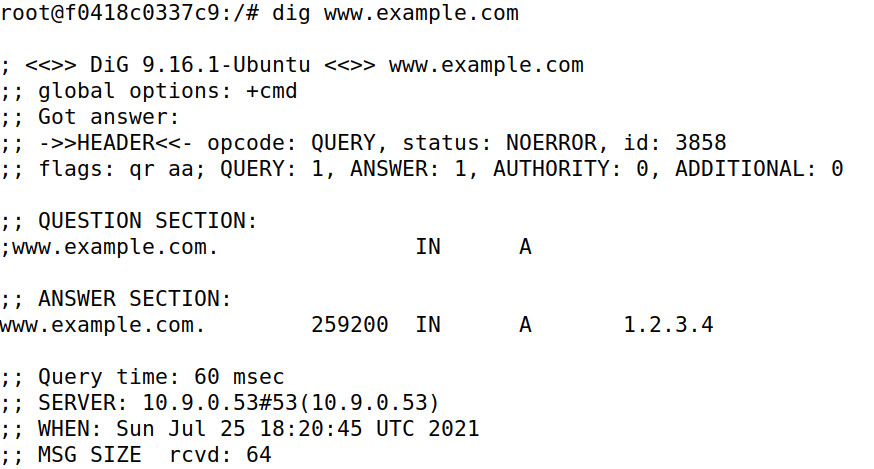
首先在靶机中dig，结果如下



发现网址被正常映射。在攻击者运行如下代码



之后再在靶机中dig，结果如下



发现网址被映射成1.2.3.4，攻击成功

**Task2**

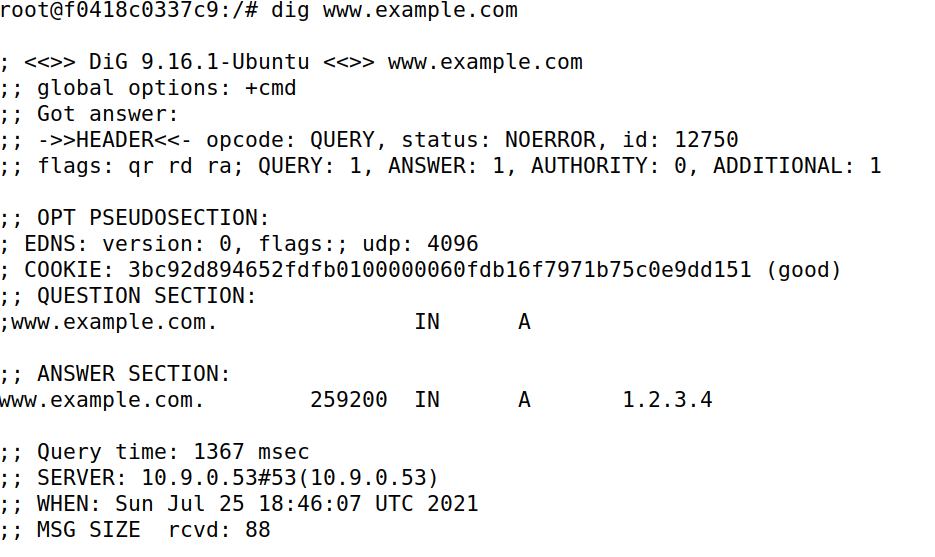
在域名服务器上清除缓存（之后每次攻击后都要清除缓存）



将代码中嗅探过滤部分中每次查询的用户改成DNS服务器，以达到持久的目的

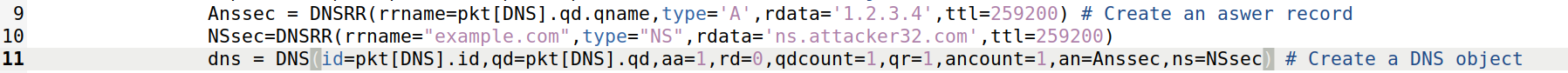


运行程序，发现攻击成功

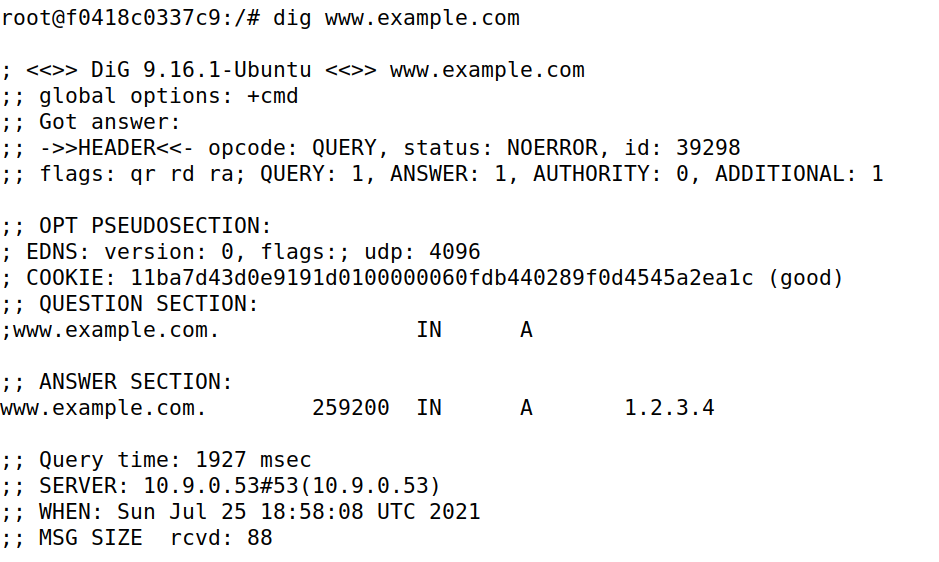


**Task3**

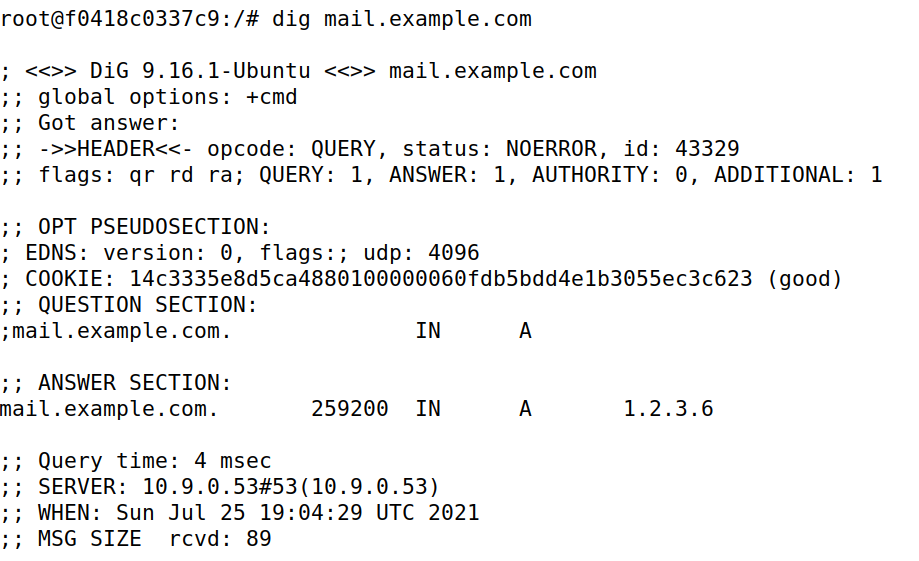
将代码修改为可以发起一次就影响整个example.com域名的攻击的形式



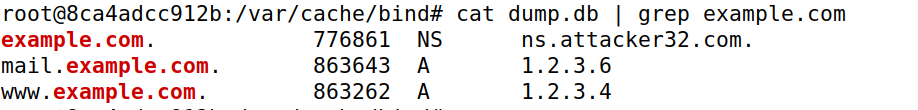
运行代码，攻击成功



且域名中如mail.example.com也被映射为其他地址

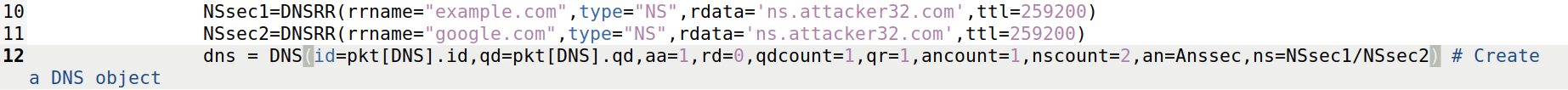


ns.attacker32.com成为example.com域的域名服务器



**Task4**

在代码增加一条google.com的条目



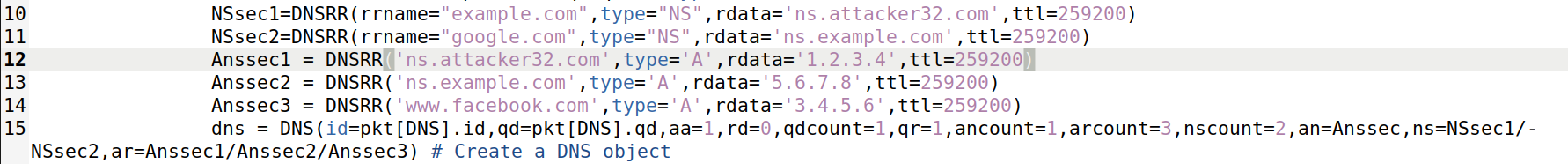
运行后发现example.com被成功的映射但无法查询google.com的映射



是因为受害者主机访问的是example.com域内的主机，故本地DNS服务器会将其储存，而google.com不在域中，故本地DNS服务器不会将该伪造报文接收，故ns.attacker32.com不会成为哦google.com的域名服务器

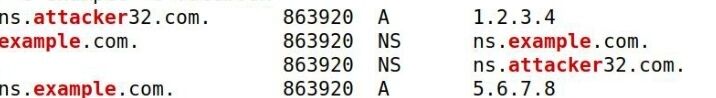
**Task5**

在代码中添加如下条目



运行后发现映射成功

查询DNS服务器缓存，记录如下



[www.facebook.com](http://www.facebook.com)不在域中，会被丢弃，故只有以上两条记录