ICS

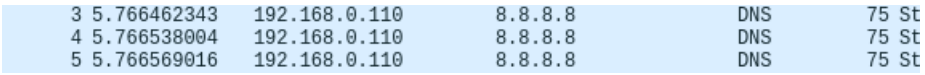
0510645

Item1.

VM's ip **:** 192.168.187.128

Victim's ip: 192.168.0.110

Commond ./dns_attack 192.168.0.110 80 8.8.8.8 on my VM and get three packet from VM's wireshark



3	5.766462343	192.168.0.110	8.8.8.8	DNS	75 St
4	5.766538004	192.168.0.110	8.8.8.8	DNS	75 St
5	5.766569016	192.168.0.110	8.8.8.8	DNS	75 St

And Victim's wireshark receive three DNS response from 8.8.8.8

2335985	3055.677441	8.8.8.8	192.168.0.110	DNS	271
2335994	3055.679819	8.8.8.8	192.168.0.110	DNS	271
2335997	3055.679821	8.8.8.8	192.168.0.110	DNS	271

Item2.

Set the Truncated bit 0, Recursion desired bit 1, Recursion available bit 1 to allow DNS server do recursion query and not to truncate the response message.Set query type to 255(ANY), so the response will contain all information such as A, AAAA, NS and so on.

Item3.

According to the DNS amplification attack how it works, the attacker will fake the DNS query with victim's ip address and let DNS server do recursion query to get the answer. During, the recursion, the response packet will grow bigger and bigger.

To prevent from the DNS amplification attack, one should set DNS server to only accept trusted DNS server to do recursive query while packets from other DNS servers should drop immediately. In this case, the DNS server will not be a stepping stone of a DNS amplification attack.