CSC-project1

0711529 陳冠儒

- Item 1 (10%): please give evidence that you have finished Tasks I and II (Illustrate your results based on some snapshots)

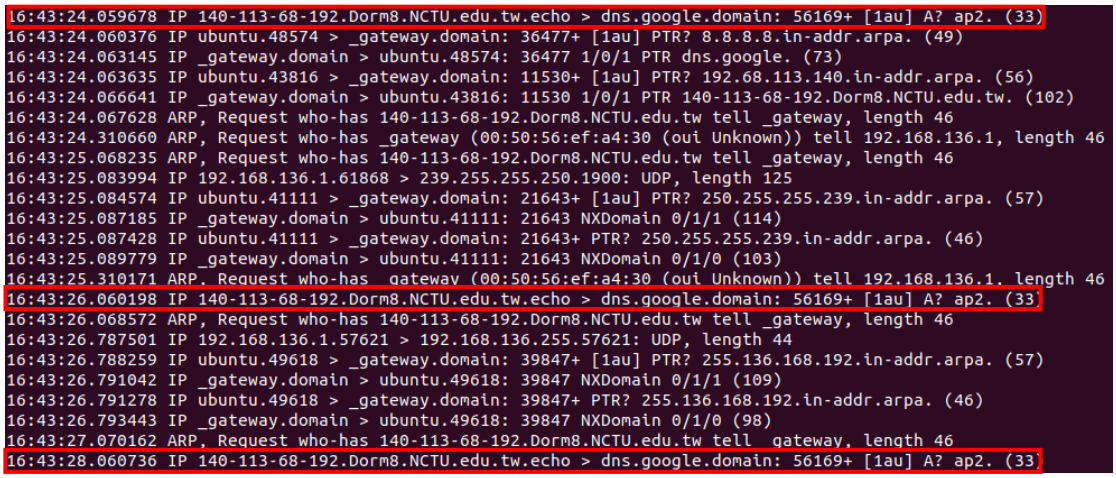

Fig 1. Attacker VMware cs2021, tcpdump -i ens33

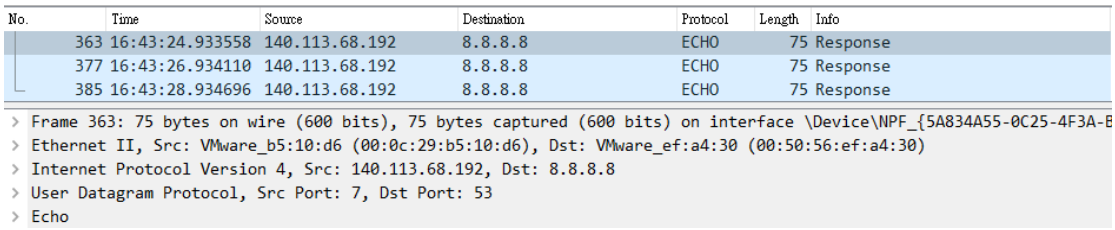

Fig 2. Attacker side, VMware Network Adapter VMnet8
(open from the victim to observe the VMware open on it)

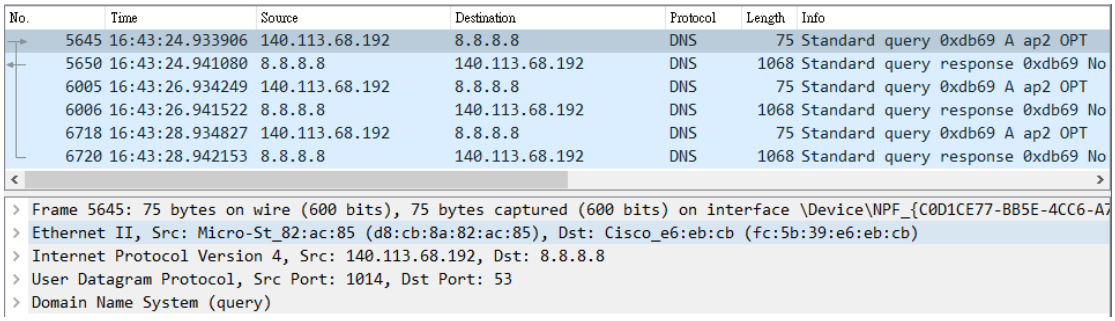

Fig 3. Victim side, wireshark ethernet

From the above three pictures, we can notice that the attacker sent the ip-spoofing dns query to dns.google.comain(8.8.8.8) and the victim received the query response after a while. The size of DNS query is 75 bytes and the size of DNS response that the victim received is 1068 bytes, so the amplification ratio is 14.24.

- Item 2 (10%): please explain how you amplify the DNS response (No more than 200 English words)

  I use EDNS to expand the UDP packet to the size of 4096 bytes, and with the DNSSEC security mechanism. DNSSEC includes the digital signature function, so there will be three more resource record types, RRSIG, DNSKEY, and DS. Among them, RRSIG is a place where the digital signature is recorded, so it has a relatively large size. With DNSSEC, each response of the DNS will have an RRSIG attached. Therefore, the more responses in one query, the larger the DNS query. After I tried it with dig, I found that querying a wrong Top-Level Domain would get the largest packet. Because after it was not found in a Root Domain, the Root Domain would find the first one in the dictionary order of the Top-level Domain (aaa). After finding that it (aaa) is wrong, it will look for the one in Top-level Domain in the dictionary order before the domain we asked, e.g. ap2(wrong one which we asked) > ao1(correct one), and it will end if it is wrong.

- Item 3 (10%): please propose a solution that can defend against the DoS attack based on the DNS reflection (No more than 200 English words)

  I think the best way to prevent DNS reflection attacks is to let the ISP prohibit any internal IP address from being spoofed. When a data packet is to be sent, if its source address is different from the internal IP, it may be that an IP address has been spoofed. There may still be some DoS attack packets that have escaped the above preventions, so the second layer of protection is that if the same query has already been sent to the response, it must wait for a mandatory TTL before sending it again, which can avoid many of the same DNS query attack. But what if the queries used in DoS attack are not all the same? I think the last layer of protection is to reduce the upper limit of DNS service speed. As a result, even with DNS attacks, other network services are still unlikely to be affected, but it is inevitable that users' inherent requests for DNS will be affected.