12.4 Question 4

12.4.A Is the web server 141.9.7.111 from question 1 susceptible to a distributed ICMP denial of service attack coming from an external network? Justify.

No, it is not as the only ICMP packets that are accepted by the network's firewall are generated by the network with the IP address 152.4.8.0/30. All other packets that are of the icmp protocol are dropped. Therefore a distributed ICMP DDoS attack would not have a great affect of this particular company network.

12.4.B Various Questions

Explain the principle of an amplification DoS attack

In amplification DoS attacks the attacker exploits the vulnerabilities in DNS servers in order to turn small queries into much larger payloads, hence, overloading and bring down the victim's server. In order to perform such an attack the attacker sends out a DNS query using the victim's IP address to an open DNS resolver. The DNS resolver than should reply to the victim's IP address. As many of these fake queries are sent out and the various DNS resolvers reply back to that one IP address the victim's network gets overwhelmed.

Give an example of an application-layer protocol which can be used for performing such attack

In order to amplify a DNS attack either the EDNS0 DNS protocol can be used as it allows for large DNS messages. Additionaly the cryptographic feature of DNSSEC can be used in order to increase the message size.

Who plays the reflector role in your example?

The reflectors in this example are the DNS resolver as these are responding to the various requests made by the attacker and send out the messages to the victim's IP address.

Find an example of an amplification DoS attack from the past

In December 2020 Citrix ADC and Citrix Gateway were targets of a DTLS amplification DDoS attack. However, the effect of this attack only appeared to be more prominent on connections with limited bandwidth.