DNS Reflection and Amplification Attacks

As with UDP flood, DNS reflection attacks use a form of IP spoofing, changing the source address in their DNS queries to show the address of their intended target, such as a DNS root server or a top-level domain (TLD) name server operator. DNS reflection and amplification recognizes UDP as an asymmetrical protocol (small requests, large responses) and the existence of open DNS resolvers to the Internet cloud. The result is that small DNS queries reflect large UDP datagram responses to the target address in the original source datagrams. Some recent attacks have used this DDoS technique at a huge scale.

Because DNS runs over UDP and does not require a handshake, it is possible to use the protocol as a means to lock down a host or a network. Designed a specific way, sending a small query to any open DNS resolver can result in a single response containing several kilobytes or more, that are sent to the unwitting spoofed victim. (This type of response typically is sent via TCP, as UDP does not allow for more than 512 bytes in a response datagram. The resulting packet usually exceeds the MTU of the recipient's interfaces, resulting in further packet fragmentation and processing.) Open DNS resolvers may allow for launching DDoS attacks containing hundreds of gigabytes of data. Attackers may also use the EDNS0 DNS protocol extension as a means to enable larger DNS responses. Many network operators, particularly overseas, allow open DNS resolvers to run on their networks, unwittingly allowing attackers to abuse them. Many network operators do provide intelligent rate-limiting to prevent abuse, even while supporting open recursive DNS servers. Hence, issues of this type usually result from mistakes in configuration.