UDP Flood

What is UDP Flood?

"UDP flood" is a type of Denial of Service (DoS) attack in which the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams.

The receiving host checks for applications associated with these datagrams and—finding none—sends back a "Destination Unreachable" packet. As more and more UDP packets are received and answered, the system becomes overwhelmed and unresponsive to other clients.

In the framework of a UDP flood attack, the attacker may also spoof the IP address of the packets, both to make sure that the return ICMP packets don't reach their host, and to anonymize the attack. There are a number of commercially-available software packages that can be used to perform a UDP flood attack (e.g., UDP Unicorn).

Attack description

User Datagram Protocol (UDP) is a connectionless and sessionless networking protocol. Since UDP traffic doesn't require a three-way handshake like TCP, it runs with lower overhead and is ideal for traffic that doesn't need to be checked and rechecked, such as chat or VoIP.

However, these same properties also make UDP more vulnerable to abuse. In the absence of an initial handshake, to establish a valid connection, a high volume of "best effort" traffic can be sent over UDP channels to any host, with no built-in protection to limit the rate of the UDP DoS flood. This means that not only are UDP flood attacks highly-effective, but also that they could be executed with a help of relatively few resources.

Some UDP flood attacks can take the form of DNS amplification attacks, also called "alphabet soup attacks". UDP does not define specific packet formats, and thus attackers can create large packets (sometimes over 8KB), fill them with junk text or numbers (hence the "alphabet soup"), and send them out to the host under attack.

When the attacked host receives the garbage-filled UDP packets to a given port, it checks for the application listening at that port, which is associated with the packet's contents. When it sees that no associated application is listening, it replies with an ICMP Destination Unreachable packet.

It should be noted that both amplified and non-amplified UDP floods could originate from botnet cluster of various sizes. The use of multiple machines will classify this attack as Distributed Denial of Service (DDoS) threat. With such attack the offender's goal is to overbear firewalls and other components of the more resilient network infrastructures.

Methods of mitigation

At the most basic level, most operating systems attempt to mitigate UDP flood attacks by limiting the rate of ICMP responses. However, such indiscriminative filtering will have an impact on legitimate traffic.

Traditionally, UDP mitigation method also relied on firewalls that filtered out or block malicious UDP packets. Yet, such methods are now becoming irrelevant, as modern high-volume attacks can simply overbear firewalls, which are not designed with overprovisioning in mind.