DNS Amplification Attack

A sort of **Distributed Denial of Service (DDoS)** assault known as a **DNS amplification attack** uses DNS protocol flaws to massively increase the volume of traffic directed at a specific server or network.

Here is a detailed explanation of a DNS amplification attack's process:

1. The attacker locates DNS servers on the internet that are weak and can be utilised to increase traffic.
2. By forging the originating IP address of the victim server or network, the attacker sends a DNS query to the weak server.
3. The victim server receives a significant amount of data from the DNS server in response to the query that is many times bigger than the initial request.
4. Because of the overwhelming volume of traffic, the target server is slowed down or sometimes crashes, making it unavailable to legitimate users.
5. The attacker can continue the assault by sending spoof DNS requests to the exposed server, which will divert increasing amounts of traffic to the victim server.

Server administrators have several options for preventing DNS amplification attacks, including:

1. To restrict the volume of data they can send to a single source, they can implement DNS Response Rate Limiting (RRL) or source address validation (SAV) on their DNS servers.
2. Updating and patching DNS server software to stop known vulnerabilities from being exploited.
3. Keeping an eye on DNS traffic and configuring alarms to spot unusual traffic patterns.
4. Blocking data from IP addresses known to be malicious with firewalls or other network security tools.