Anatomy of a DDoS

In this lesson, we'll study distributed denial of service attacks.

We'll cover the following

What is a DDoS attack?

A DDoS attack is a special type of offense that a malicious user throws against you. It generates an incredible amount of traffic towards your servers so that they can no longer accept genuine traffic, rendering your service unavailable.

What is a DoS attack?

The simplest form of a DDoS attack is a DoS, otherwise known as, you guessed it, Denial of Service. This attack is, fundamentally, a DDoS without being distributed, meaning that the source of the attack is fixed, a machine that repeatedly sends traffic to a network, attempting to bring it down.

Blocking a DoS attack is usually a simple task, as one could simply create a firewall rule banning the IP address that generates the disproportionate amount of traffic. DoS attacks are generally easier to mitigate, therefore we’ll simply refer to DDoS throughout this chapter, as we believe they are a much bigger threat to our web applications than DoS. A large portion of the mechanics behind them are exactly the same, with the only difference being the originator(s) of the attack. A DoS is a machine attempting to bring down a server through network requests, a DDoS is multiple machines performing a DoS.

A helpful metaphor

Imagine a new bridge is inaugurated in Securityville and you really, really dislike Securityville's head of traffic department. What you could do is call all of your friends and ask them to slowly drive on the bridge, bringing traffic to a standstill. Other drivers won't be able to use the bridge since they're stuck in traffic, and the head of the traff will be furious as his creation is not helping, but rather creating congestion.

traffic on a bridge taken from:
https://commons.wikimedia.org/wiki/File:Morning_traffic_on_the_Golden_

Now, replace the bridge with webservers, drivers with web surfers, and your friends with thousands of machines you control and you have a DDoS attack. You flood a network with incoming traffic from your own machines until the network is so overloaded it can't serve any more requests, affecting a genuine user's ability to access the network.

The simplest DDoS attack

The simplest form of a DDoS attack is a DoS, otherwise known as, you guessed it, Denial of Service. This attack is, fundamentally, a DDoS without being *distributed*, meaning that the source of the attack is fixed, a machine that repeatedly sends traffic to a network, attempting to bring it down.

Blocking a DOS attack

Blocking a DoS attack is usually a simpler task, as one could simply create a firewall rule banning the IP address that generates the disproportionate amount of traffic. DoS attacks are generally easier to mitigate, therefore we'll simply to refer to DDoS throughout this chapter, as we believe they are a much bigger threat to our web applications than DoS, even though a large portion of the mechanics behind them are exactly the same with the only difference being the originator(s) of the attack. A DoS is a machine attempting to bring down a server through network requests, a DDoS is multiple machines performing a DoS.

A DDoS attacker doesn't have to generate a lot of traffic

traffic

There are different types of DDoS attacks, so all you need to remember is that their goal is to overload your webservers by exploiting a vulnerability in your network. That vulnerability could be anything, from the fact that your network is open to the public to an actual technical vulnerability such as slowloris.

Remember when I said that in a DDoS an attacker generates an incredible amount of traffic towards your servers? I kind of lied to keep it simple; an attacker doesn’t always have to generate incredible amounts of traffic but can simply exploit a vulnerability to bring your service down.

When we think of DDoS we tend to associate them with large amounts of bots sending traffic to our servers, while in some cases a handful of machines can easily take us down with a few hundred requests.

Slowloris: an example

Again, taking slowloris as an example, it exploits a vulnerability in web servers where connections are never closed as the client keeps sending small packets of data to the server, making it believe the client is alive and well, just slow to send packets.

The server allocates resources for each client request but will run out of them after N parallel slow requests are in progress. If the number of slow requests exceeds the maximum number of threads the webserver is configured to create, the attack is successful; the webserver is forced to drop genuine traffic while processing the slow, malicious requests.

I wanted to mention slowloris as it belongs to a particular class of DDoS attacks called “low and slow”, and not the more traditional brute-force kind of attack we’re used to thinking of when DDoS is mentioned. This goes a long way to show you that there are a lot of things to consider when worrying about DDoS attacks. It’s not just about blocking large amounts of traffic suddenly coming at us.

As we will see later in this chapter, your best bet is to rely on an external provider, rather than building a wall yourself that will inevitably crumble.

In the next lesson, we’ll study why anyone would want to take your website down.