NimbusDDOS

ARTICLE :

Simulated Attack FAQ

A simulated attack can help you be prepared for a DDoS attack. However, many customers have concerns about such attacks, since they are, after all, real attacks on their platform. What are the risks?

In this article, we will discuss the frequently asked questions about simulated attacks and why clients shouldn't be intimidated. In fact, when we identify weaknesses and fortify your system, it's the DDoS attackers who should become worried!

Learn more about the philosophy, mechanics and safety of our simulated DDoS attacks below.

The Philosophy

Getting familiar with the concept of a simulated attack is important before delving into the mechanics and other concerns about the process.

- "What is a simulated DDoS attack?" A simulated DDoS attack is a controlled, strategic, real attack on your environment with the aim of proactively finding weaknesses in your infrastructure that are vulnerable to DDoS attacks.

- "Why would I want to attack myself?" Preparation is key for DDoS attacks. Protection requires a custom plan based on your environment, mitigation systems, and incident response team who will carry out the tasks necessary to mitigate an attack. Coordinating these components and identifying gaps is best done in a controlled, proactive exercise that closely matches a real-world DDoS attack.

The Mechanics

Understanding how a simulated attack works can helps clients feel more confident in this type of testing. Many have questions about which attack vectors will be used, where they are run, and how a simulation is different from other testing.

- "Where do we run the simulated DDoS attacks?" Like a real attack, our simulated DDoS attacks are sourced from around the world. We do this by leveraging the resources of public cloud vendors.

- "What simulated DDoS attacks should I perform?" The attack vectors for your system are contingent on the risk areas in your environment. Generally, a risk assessment is conducted beforehand and the results indicate which types of attack vectors should be executed on your specific systems. A DDoS expert will guide the selection to maximize the value of the test and the usefulness of the data collected.

NimbusDDOS

- "How are simulated DDoS attacks different from load testing?" A load test helps identify the upper limit of your system's capacity with normal traffic. A DDoS attack can involve traffic with tens of thousands times more traffic than is normal. Also, the attack may use protocols and traffic pattern behaviors that aren't typical of normal use, to target specific DDoS attack risk areas.

The Safety

Test are often run against the production portion of a client's environment. As a result, clients often have questions regarding the safety of this type of testing. Some of the most common questions are answered below, but rest assured that our DDoS experts have extensive experience in safely performing these tests against environments with even the strictest availability requirements.

- "Is it legal to perform simulated DDoS attacks?" Our position is that a simulated DDoS attack is legal when performed in a responsible manner.

- "Do the simulated DDoS attacks have an emergency shutoff?" Indeed. We employ two mechanisms that can shut down any attack in less than a minute. The first is an in-band mechanism (that uses NimbusDDOS communication pathways) and the second is an out-of-band mechanism (using cloud vendor pathways).

- "How are simulated DDoS attacks sized?" To limit the impact to the client's environment, we work closely with the client's team to size tests appropriately. By setting the appropriate size we are able to minimize unexpected impact, while still designing a meaningful test. Additionally, the NimbusDDOS testing platform is capable of very precise traffic delivery that can be slowly increased to minimize risk to the environment.

Staging a Simulated Attack with NimbusDDOS

As you can see, a simulated attack is a systematic, safe and beneficial method to help proactively protect your business from DDoS attacks. Especially during these unprecedented times, a pause to your revenue, or extortion attempt due to a DDoS attack - or threat of attack - could be devastating. Your cybersecurity should be a higher priority than ever.

Are you interested in staging a simulated attack to help protect your system from such an event? Contact NimbusDDOS or call (800) 674-DDOS.