LODDOS

DDoS Attack Test Platform

loddos-sec.com

LODDOS

WHY PERFORM DDoS TESTS?

In practice, DDoS tests are performed to assess the efficiency and the limits of the DDoS prevention products and services in place, to improve these systems and related precautions, as well as to measure and enhance the efficiency and the capabilities of an organization, within the assumption of a DDoS attack.
DDoS prevention solutions are not designed to work in a plug-and-play set-up.

Hence, prior to taking the necessary safety measures, an organization's normal and abnormal network traffics, baselines and thresholds must be determined.

To identify these crucial elements properly, engineers should test the already-protected services against a real time DDOS attack and should also conduct some research on the current DDoS attack solutions within the market.

HOW TO PERFORM DDoS TESTS?

As of now, most DDoS tests are being executed manually. The technical and administrative preparation stages of these tests take way too long than usual. Security and IT teams must work concurrently for a considerable amount of time to configure on premise traffic generator systems to conduct DDoS tests. Moreover, the operational aspect of this preliminary work also consumes additional load of time and cost, too.

Real-time monitoring of DDoS tests is usually not available during these manual tests, and it takes a significant amount of time to generate reports once the test phase is completed. Even if the test phase is done, predominantly these reports are not re-usable.

2018 Corero Trends Report

95% of the DDoS episodes performed are 5 Gbps or less in size. The rate of attacks on 10Gbps is **2%.**

NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report

75.7% of the DDoS attacks performed are volumetric attacks.

End Users, Financial Services, Cloud Services, and Public Services are the targets that are subject to DDoS attacks respectively.

The cost of a successful DDoS attack on the target organization varies between **$10,000** and **$100,000**

WHAT IS LoDDoS?

LoDDoS is a DDoS and Load Test simulation platform offered as a service via cloud. The platform generates real DDoS attacks against services via real attack parameters. It also evaluates the resilience of internet-enabled web applications against high traffic.

This enables organizations to test the limits and the efficiency of their existing DDoS prevention systems prior to an actual DDoS attack. The tests which are defined on LoDDoS, are conducted with the attendance of an Operator as well as can be initiated with a single action, monitored live, stopped in a controlled manner, repeated as often as needed. Reports can be generated automatically and promptly by the end of each test thus results can be shared with third parties, if requested.

DDoS test sessions in LoDDoS platform can be monitored in real-time by all parties and can be paused at any time in case of an emergency. All tests can be repeated, and the results can be compared. Reports are generated instantly and can be saved for later evaluation.

A high number of requests targeted to web applications can be addressed with the help of LoDDoS's Load Test feature, thus the limitations of these applications become visible. Load Test paves the way to analyze real situation that creates a considerable amount of load on applications before it occurs.

LoDDoS ARCHITECTURE

LoDDoS contains three main components. These components are;

1. Command-and-Control Center - *where the attacks performed are defined, managed, monitored and reported,*
2. Bot Networks- *where the attacks are conducted,*
3. Monitoring System - *where the target system's health status is monitored.*

Command-and-Control Center is governed via a web interface. There are different user roles pre-defined for management, operations, and monitoring. DDoS tests are conducted following a two factor security authorization phase. Bot Network runs on a cloud service provider and all bots are administered via Command-and-Control Center. Metrics such as the number of bots within the bot network, the geographical location and the bandwidth generated within the session can be all controlled via Command-and-Control Center based on the scope of each test.

LODDOS

SUPPORTED DDoS ATTACK TYPES

The main purpose of supported DDoS attacks is to exhaust the network and system resources of the targeted destinations and to prevent these systems from being operational.

Principally, it is intended disable the resources by sending packets more that exceeds the current Internet bandwidth of the targeted systems.

TEST TYPE	DESCRIPTION
TCP SYN Flood (Layer 4)	The aim of a TCP SYN Flood attack is to exploit a TCP three-way handshake process by sending a substantial volume of SYN flagged TCP packets to the targeted server.
TCP SYN-ACK Flood (Layer 4)	In TCP SYN-ACK Flood, a substantial volume of SYN/ACK flagged TCP packets are sent to the target. Out-of-state SYN/ACK packets violate three-way handshake process.
TCP ACK-FIN Flood (Layer 4)	In TCP ACK-FIN Flood, a substantial volume of ACK-FIN flagged TCP packets are sent to the target. Out-of-state ACK-FIN packets violate TCP connection termination process.
TCP RST Flood (Layer 4)	In TCP RST Flood, a substantial volume of RST flagged TCP packets are sent to the target server. Targeted server goes through all of it's transmission list in order to response to incoming requests.
TCP PUSH ACK Flood (Layer 4)	In TCP PUSH ACK Flood, a substantial volume of PSH-ACK flagged TCP packets are sent to the target server. PSH flag signals the server to bypass TCP buffer and to directly transmit it to the running service.
TCP All Flags Flood (Layer 4)	Also known as Xmas Flood, in TCP All Flags Flood a substantial volume of TCP packets are sent with all TCP flags (SYN-ACK-FIN-RST-PSH-URG) present in it's body.
TCP No Flags Flood (Layer 4)	Also known as TCP Null Flood, in TCP No Flags Flood a substantial volume of TCP packets are sent with no TCP flags.
UDP Flood (Layer 4)	Aim of UDP Flood is to saturate bandwidth and consume the resources of the targeted server by sending a substantial volume of UDP packets.
UDP Fragmented Flood (Layer 4)	Similar to the UDP Flood, UDP Fragmented Flood aims to waste resources of the targeted server by sending a substantial volume of fragmented UDP packets of the maximum size, in order to saturate the channel with as few packets as possible.
ICMP Flood (Layer 3)	Aim of ICMP Flood is to disrupt a server's ability to use ICMP(Ping, Echo Request), by saturating it's bandwidth with a substantial volume of ICMP packets.
SSL Negotiation Flood (Layer 6)	SSL Negotiaton Flood aims to render a SSL/TLS service unresponsive by establishing disproportionate SSL handshake with targeted server, as a SSL/TLS handshake is a lot more CPU intensive on the server side than on the client side.
HTTP(S) GET (Layer 7)	Aim of HTTP(S) GET attack is to simulate a high number of real users requesting the resources of a web application by sending a substantial volume of HTTP(S) GET requests.

LODDOS

TEST TYPE	DESCRIPTION
HTTP(S) POST (Layer 7)	Aim of HTTP(S) POST attack is to simulate a substantial number of real users sending data to the web application by directing a high number of HTTP(S) POST requests with customizable payload to the application.
Slowloris (Layer 7)	The aim of the Slowloris attack is to fill the maximum concurrent connection pool of an application with minimal bandwidth usage by establishing various connections on the server and keeping these connections valid as long as possible.
DNS Query (Layer 7)	In DNS Query Flood, a substantial amount of DNS queries are sent to a DNS Server in order to saturate the bandwidth and consume the resources of the DNS server.
DNS Random Query Flood (Layer 7)	Similar to the DNS Query Flood, a substantial amount of DNS queries are sent to a DNS server in order to saturate the bandwidth and consume the resources of the DNS server.

Test Volumes

#Bots	L3/4 Tests (Volumetric) Bandwidth MBPS (upto)	L7 Test (Application) Running User (upto)
50	3.000	500.000
200	12.000	2.000.000
400	24.000	4.000.000
600	36.000	6.000.000

SECURITY

2-Factor Security

To conduct a DDoS test; both the operator (the Tester) and the client (the Target) should mutually approve the execution. Thereby, the scheduled test is guaranteed to be performed once the consent process is completed.

Emergency Stop Button

The tests being conducted can be paused with a click of an emergency button, if desired. In case of unexpected and extraordinary situations, tests can be stopped deliberately and resumed at any time.

LOADDOS

DDoS Attack Test Platform