RED BUTTON
DDoS Experts

DDoS Penetration Test Service

How do you know if your DDoS mitigation can stand in the face of a real DDoS attack? Can you estimate how long will it take from the moment an attack is launched till you are able to detect it and begin resolving it? Strategy and planning are critical, yet to really ensure your mitigation provides the right protection, you must test it under a realistic DDoS attack.

RedButton's DDoS Penetration test service enhances your DDoS readiness by simulating attacks in a secured, controlled manner. Using proprietary cloud technology, our penetration test specialists generate multi-vector DDoS attacks and try to breach your defense systems.

With our DDoS Penetration Test service, you:

- Realistically asses your DDoS protection readiness, prior to a real attack
- Identify weakness points and improve your protection level
- Increase your confidence level for the day of a real attack
- Drill your engineering teams and managers

Types of Attacks Generated

Building on our expertise protecting against hundreds of DDoS attacks, we generate realistic attacks simulating the most recent attack trends. Your system will be tested for the following attack categories:

Volumetric DDOS attacks:

Our platform can generate a multi-gigabit attack traffic from multiple global locations, testing your ability to withstand extreme and sustained throughput, connection and packets loads. We apply the same load patterns as attackers, such as large UDP packets and SYN flooding.

Application layer DDOS attacks:

We use our testing platform to overwhelm your web server tier, generating excessive HTTP/S GET or POST requests to selected URLs in order to test your resistance to resource exhaustion.

Low-and-slow attacks:

Attackers can create extremely effective attacks using very low resources, such as DNS, SMTP or NTP amplification/reflection attacks. Our DDOS Penetration test plans include similar test scenarios to verify that your infra-structure is protected against such unexpected vulnerabilities.

info@red-button.net www.red-button.net +972-77-320470 +972-54-5555983

RED BUTTON
DDoS Experts

How We Perform Attacks

Our simulated DDoS attacks are both legal and safe. All attacks require customer in-writing consent and performed based on planning session goals and agreed-upon schedule. To perform attack we use dedicated co-located servers (with absolutely no compromised hosts), and agents distributed globally. We use our management console to control attacks and in case of need, an emergency Stop button can instantly kill a simulated attack.

PLANNING SESSION

During this phase we meet with your team to understand the structure of your system, assemble technical details, define clear goals and the exact schedule of the test.

CONTROLLED DDOS ATTACK

ABased on the defined goals, we launch multi-vector DDoS attacks that can include any combination of volumetric attacks, application-layer attacks and Low-and-Slow attacks. The test last between 2 to 6 hours.

SUMMARY & RECOMMENDATION

The summary phrase includes a f2f meeting and a written report summary, outlining the effectiveness of your existing DDoS mitigation solution. The report points out vulnerabilities within your infrastructure and provides recommendations on how to amend them.

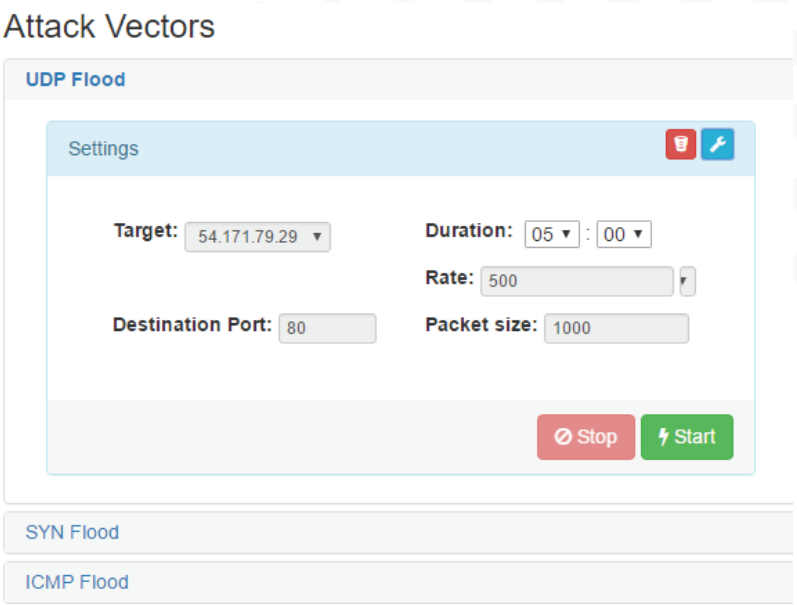
Provider/ criteria	RED BUTTON DDoS Experts	Other service's providers
Total DDoS Service	The DDoS Simulation will reveal to many organization that they have gap to cover. Red Button does not stop there and offer all the tool and services to close the gap and continue with the customer the entire DDoS cycle. This includes architecture, vendor selection, training, and more.	For many provider's DDoS is not the main focus of the company and they do also vulnerability assessment and phishing simulation. They will not provide consulting, training, and DDoS fully managed services, and after the test you are basically on your own.
Standard-Based	Red Button uses the DDoS Resiliency Score (DRS) which is an open standard, facilitating an objective result.	Other DDoS providers either do not have a test standard at all or alternatively use a proprietary closed standard that neither you nor the entire industry can challenge.
Virtual DDoS Simulation	Not always you can put all your assets into a DDoS Simulation. In this case Red Button offers a unique "virtual" DDoS Simulation tool that can tell you where you stand in a white-box "dry" approach.	

info@red-button.net www.red-button.net +972-77-320470 +972-54-5555983

RED BUTTON
DDoS Experts

DDoS Simulation - Do It yourself

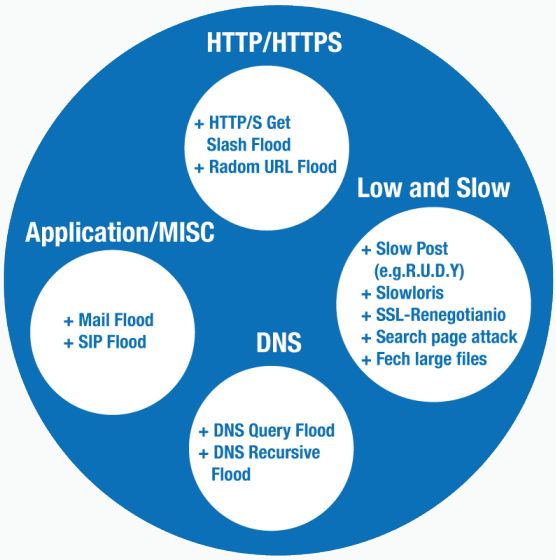
OThe DDoS Simulation DIY is a service for large organizations and security consultants that do more than one test an year, and wish to control directly the DDoS test - a most recommended action by us, which also as a side effect reduce costs.
The DDoS Simulation Platform allow anyone with technical skills to operate access or intuitive user interface and run attacks safely



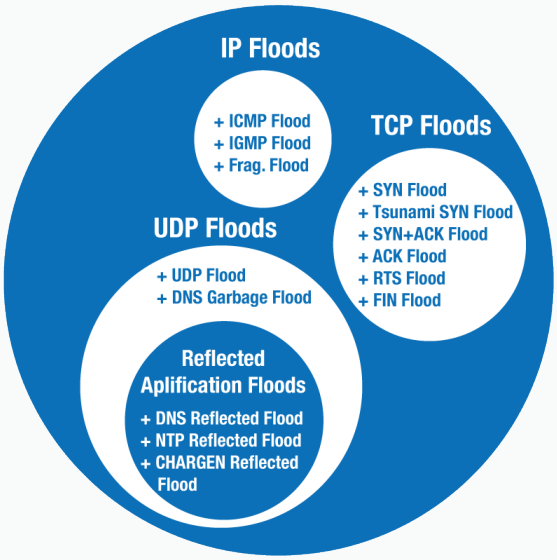
Attack Vectors Perspective

Our DDoS Simulation covers the following Attack Vectors: Based on the defined goals, we launch multi-vector DDoS attacks that can include any combination of volumetric attacks, application-layer attacks and Low-and-Slow attacks.

Application Floods



Network Floods



info@red-button.net www.red-button.net +972-77-320470 +972-54-5555983

RED BUTTON
DDoS Experts

Q&A

How does DDoS Simulation work?

DDoS Simulation also called DDoS Pen Test is a ready DDoS attack that is conducted in except that it is being done in a very controlled manner. The attack vectors are launched from a legitimate botnet. Typical attack will include half a dozen attack vectors and a prolong attack may include a dozen attack vectors.

What is the difference between real attack and DDoS attacks?

	Typical Severe DDoS Attack	DDoS Simulation
Attack vectors	Multiple	Multiple
Attack volume	Very high	Very high
Botnet type	Malicious botnets	Legitimate botnet induced on legitimate resources
Who controls the attack	Attacker	We
What happen if there is an impact	Attack continues, this is the point of the attacker	Immediate halt, the failure is logged and alter fixed.

How is it priced?

The attack price is based on attack duration and attack volume primarily. A 6 hours DDoS simulation will be more expensive than 3 hours, and a 10Gbps will be more expensive than 1Gbps. Please request a quote to proceed.

Is it legal?

Yes. On our side we have taken all steps to ensure the legality of the test, and use only legal resources. On the customer side there are several steps to ensure the legality. The customer most grants us permission to make the test and must inform the ISP and hosting service prior to the test.