P.O.B. 42, Tel-Aviv, Israel +1-201-564-1126 sales@red-button.net red-button.net

RED BUTTON
DDoS Experts

RED BUTTON DDOS TESTING

- RB- TEST-3H-6V
- RB-TEST-6H-12V
- RB-TEST-3H-6V-ANALYSIS
- RB-TEST-6H-12V-ANALYSIS

Services Family

YOUR DDOS READINESS BEGINS WITH EFFECTIVE DDOS TESTING

How can you be sure your DDoS mitigation solution can withstand a full-blown, multi-vector DDoS attack?

Can you estimate how long it will take to detect a stealthy application layer attack and begin resolving it?

DDoS Testing services help you verify the effectiveness of your DDoS mitigation strategy by simulating real-world DDoS attack scenarios.

Test your systems against the most dangerous attack vectors

Understand test results and identify reasons for gaps

Translate analysis into doable actions and practical recommendations

Implement the right solutions at the right time

But DDoS testing is only one step in your journey towards complete DDoS readiness. Knowing the test results is of little value if you can't translate those results into actionable recommendations to improve your security posture. Red Button's DDoS Testing service is uniquely equipped to do just that. In addition to executing deep multi-vector DDoS testing, Red Button's DDoS experts provide a full range of complementary services that optimize your mitigation practices and maximize DDoS resiliency.

DDOS TESTING FOR ALL TYPES OF ATTACKS

Building on our unmatched expertise in mitigating hundreds of DDoS attacks, Red Button simulates realistic attacks based on the latest attack trends. We test against the following attack categories:

Volumetric Attacks

Using proprietary cloud technology, the DDoS Testing service can generate multi-gigabit attack traffic from multiple global locations, testing your ability to withstand extreme and sustained throughput, connection and packet loads. These tests apply the same load patterns as attackers, such as large UDP packets and SYN flooding.

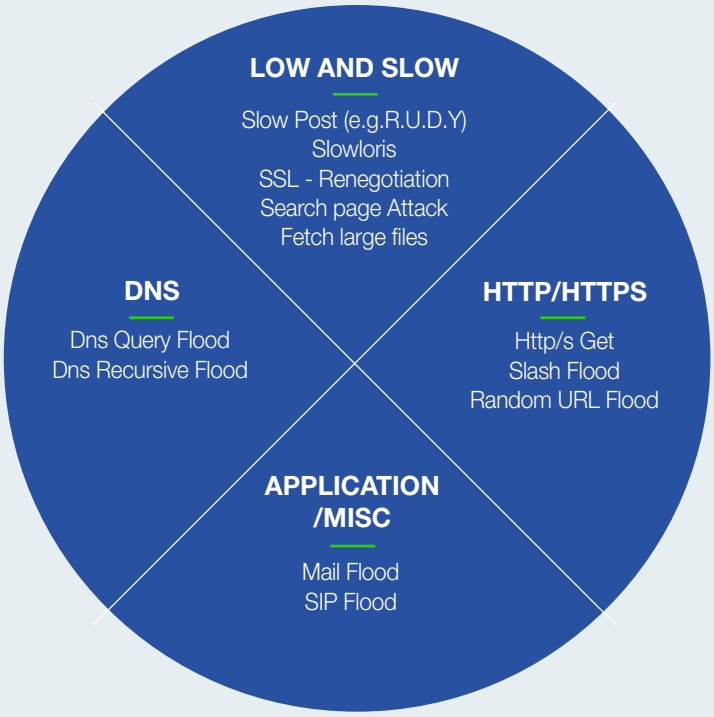
Application Layer Attacks

Red Button's testing platform generates traffic to overwhelm your web server tier, such as excessive HTTP/S GET or POST requests to selected URLs that test your mitigation solution's resistance to resource exhaustion.

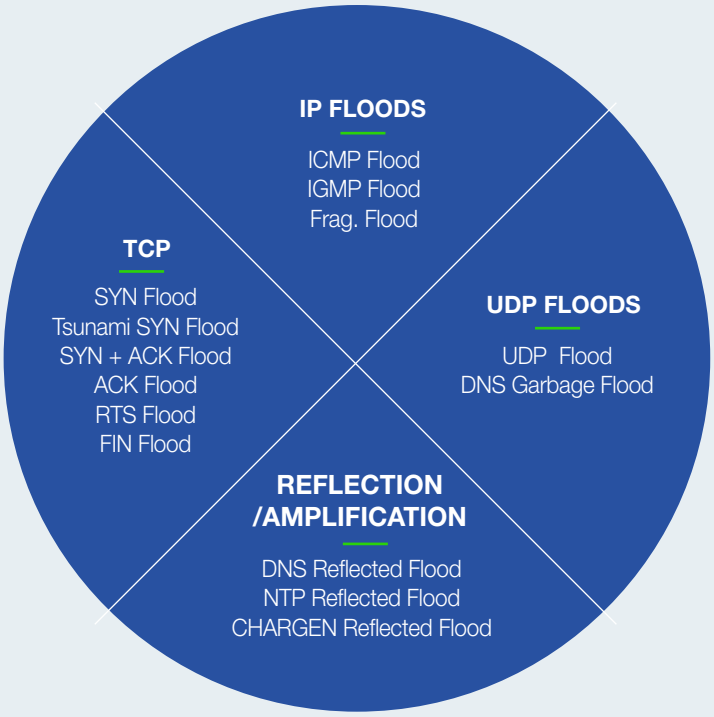
Low-and-slow Attacks

These attacks, such as SlowLoris, R.U.D.Y., and SSL-Renegotiation are hard to detect because they use low resources. The DDoS Testing service includes "low-and-slow" test scenarios to verify that your infrastructure is protected against such unexpected vulnerabilities.

APPLICATION FLOODS



NETWORK FLOODS



HOW WE PERFORM ATTACKS

Red Button's simulated DDoS attacks are both legal and safe. All attacks require written customer consent and are performed based on planning session goals and an agreed schedule. Attacks are securely executed using dedicated servers (with absolutely no compromised hosts) and globally distributed agents. Attacks are controlled and monitored using our management console, including an emergency Stop button to instantly kill a simulated attack if needed.

PLANNING SESSION

Red Button experts meet with your team to understand your network architecture, assemble technical details, define clear goals and test schedule. This includes planning the DDoS test scope and targets, attack vectors, and attack rates. The joint planning effort is detailed in the DDoS Test Plan document

CONTROLLED DDoS ATTACK

Based on the defined goals, Red Button launches multi-vector DDoS attacks that may incorporate any combination of volumetric attacks, application-layer attacks and Low-and-Slow attacks. The test typically lasts between 3 to 6 hours.

SUMMARY & RECOMMENDATION

Red Button prepares a written DDoS Testing Report outlining the effectiveness of your existing DDoS mitigation solution. The report includes an executive summary of the test results, as well as a complete log of the simulation. In addition, the report identifies vulnerabilities within your infrastructure and provides recommendations on how to correct them.

Red Button DDoS Testing is part of our comprehensive **DDoS Readiness** program!

Upon completion of a DDoS testing and analysis session, new customers may opt-in to the DDoS Readiness program and receive **two additional testing sessions** as part of their ongoing service.

MAXIMIZE THE VALUE OF YOUR DDOS TESTING

Testing Attribute	Red Button DDoS Testing	Other DDoS Testing Service Providers
Gap analysis based on testing results	**Full gap analysis including actionable recommendations.** In addition to providing detailed test results, Red Button provides a full analysis of the test findings, including reasons for the gaps, overall score based on DRS, industry comparison, long-term and short-term recommendations. This information is included in the summary report and is also presented in-person to the customer.	**No analysis of test results.** Test summary comprises a "dry" report with a pass/fail grade for the mitigation of each attack vector. There is no analysis of the results
Full-stack DDoS services	**Deliver any related service the DDoS test shows you need.** Red Button is not only your DDoS testing provider, but your trusted DDoS services partner for the long haul. If the DDoS test reveals the need to close a technical gap, create procedures or train your personnel, Red Button has all the complementary services to do so. Our experts also provide IR services for customers under attack.	**Perform one-off DDoS penetration test without additional services.** They don't analyze or act on the findings, which leaves you on your own to close the gaps any other necessary follow-up steps.
Testing approach	**Red Button uses a “white-box” testing approach designed to enhance DDoS readiness.** We analyze the entire network architecture with the customer prior to testing and then jointly decide on the most relevant attack vectors to perform. This approach is designed to maximize the value and actionable outputs of the testing with minimum complexity and cost. In contrast to RT/BT testing, Red Button's sole objective is to improve the customer’s DDoS readiness.	
Standard-Based	**Open, standard-based testing service.** Red Button uses the DDoS Resiliency Score (DRS) which is an open standard, facilitating an objective result.	**Do not use open testing standards.** Typically do not adhere to a test standard, or alternatively use a proprietary closed standard that cannot be challenged by customers or the industry.

PRODUCT COMPARISON

Service	RB-TEST-6V-3H	RB-TEST-12V-6H	RB-TEST-6V-3H -ANALYSIS	RB-TEST-12V-6H -ANALYSIS
General test sizing				
Frequency	One-time event	One-time event	One-time event	One-time event
Attack vectors	6	12	6	12
Simulation duration	3 hours	6 hours	3 hours	6 hours
Maximal bandwidth	10 Gbps	10 Gbps	10 Gbps	10 Gbps
Maximal PPS	5M	5M	5M	5M
HTTP RPS[1]	100K	100K	100K	100K
HTTPS RPS[1]	25K	25K	25K	25K
Phase 1 - DDoS simulation planning				
DDoS Test planning	✓	✓	✓	✓
Reconnaissance	—	—	✓	✓
DDoS Test Plan document	✓	✓	✓	✓
Phase 2 - Controlled DDoS attack execution				
DDoS Testing	✓	✓	✓	✓
Phase 3 - DDoS simulation summary report				
Test summary				
Test results - summary	✓	✓	✓	✓
Test result - details	✓	✓	✓	✓
Test analysis				
Overall score[2]	—	—	✓	✓
Recommended score	—	—	✓	✓
Gap analysis	—	—	✓	✓
Industry comparison	—	—	✓	✓
Recommendations - short term	—	—	✓	✓
Recommendations - long term	—	—	✓	✓
Misc				
Submission duration[3]	10 working days	10 working days	10 working days	10 working days
Presenting result to the customer	1 meeting	1 meeting	1 meeting	1 meeting

[1] Subject to customer's service capacity
[2] Based on the DRS (DDoS Resiliency Score) open standard. For more details see www.ddosresiliencyscore.org
[3] Starting from the DDoS simulation