RED BUTTON
DDoS Experts

DDoS Course
Basics 101

“In combat, it is not enough to only have good planes, you must also have excellent pilots.”

Red Button DDoS Courses

If you want your organization to be prepared for DDoS attacks, you should know that it takes more than just procuring the right solution. Attacks are waged by people; they are also resolved by people. Thus, it is crucial for your technical peers to be trained so that they can act quickly and efficiently in identifying an ongoing attack and taking the correct measures against it.

Red Button helps security professionals attain these goals.

DDoS Course Basics 101

Course name	Red Button DDoS 101 Basic
Duration	2 days
Overview	• An introductory course to DDoS. • Understanding both DDoS attacks and DDoS mitigation technologies. • Includes both theory and DDoS labs. • Allows students to develop a mature approach toward DDoS.
Intended audience	Information security personnel, network engineers, CISOs, NOC/SOC managers, and all other IT staff who handle DDoS attacks.
Location	Red Button offices: ROOMS at NYX Hotel Tel-Aviv HaRakevet St. 29 Tel Aviv, Israel
Maximum class size	12 students
Pre-requisites:	Basic knowledge of computer network and security. Laptop.
Certification	RB-DDOS-101 (upon successful completion of the final exam)
Recommended next course	Red Button DDoS 102 Advanced

Agenda

(course agenda may change slightly from time to time)

Day I – Attacks

Time	**Duration** (min)	**Activity**
08:45-09:00	15	Gathering
09:00-09:15	15	DDoS Course Basics 101 Introduction
09:15-10:45	90	Introduction to DDoS Threat Landscape
10:45-11:00	15	Break
11:00-11:30	30	Introduction to Wireshark
11:30-12:30	60	Lunch break
12:30-15:30	180 (3 hours)	DDoS Attack Lab 1 Running DDoS attacks using the Red-Button DDoS Simulation Platform (SYN Flood, HTTP Flood, DNS Flood, Slow POST and SSL Renegotiation) and reviewing the attacks on the server-side.
15:30-17:00	90	DDoS Threat Landscape and DDoS Attacks Exercise

Day II - Mitigation

Hour	**Duration** (min)	**Activity**
08:45-09:00	15	Gathering
09:00-10:30	90	Introduction to DDoS Mitigation Technologies
10:30-10:45	15	Break
10:45-11:45	60	SYN Cookies Advanced
11:45-12:15	30	DDoS Mitigation Exercise SYN Cookies Advanced Exercise
12:15-13:15	60	Introduction to DDoS Mitigation Architecture
13:15-14:15	60	Lunch break
14:15-15:50	95	DDoS Attacks Lab 2 Running SYN Flood and HTTP Flood attacks using the Red-Button DDoS Simulation Platform and creating mitigation mechanisms against them (Proxy, Caching, Web Challenges, Geo-based Protection and Rate-limit Rules). Running raw attack commands using hping, curl and ab.

15:50-16:10	20	Break
17:00-18:00	60	Final Exam

About the Course Author

Ziv Gadot, Founder & CEO, Red-Button.

Prior to establishing Red Button in 2014, Gadot has dedicated 11 years to Radware, one of Israel's leading software security vendors. He had founded and managed Radware's Emergency Response Team (ERT), a 24x7 response team that helps organizations under DDoS attacks. Before joining Radware, Gadot held leading consulting positions with Check Point and Intel.

With a Bachelor of Arts degree in Computer Science and Master's in philosophy, Ziv is a frequent speaker at security conferences and author of several security reports and bulletins. Ziv handled hundreds of DDoS attacks and trains not only the security staff within the customer's organization, but also DDoS vendors and major service providers, including AT&T, Akamai-Prolexic, Radware, SecurityDam and many others.

About Red Button

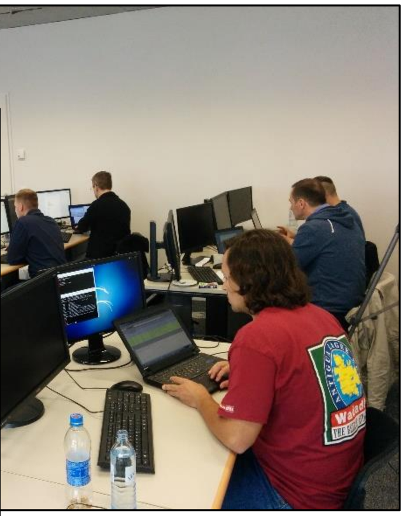
Red Button is a security services and consulting company specializing in Distributed Denial of Service (DDoS) cyberattacks. We have helped mitigate hundreds of DDoS attacks on banks, online bidding platforms, and governments, and we use our expertise to provide preemptive and emergency response services to organizations of all sizes. Our services include DDoS readiness evaluation, penetration tests, technology selection, consulting, SOC training, and emergency response. Red Button also established the DDoS Resiliency Score (DRS) standard, which helps companies evaluate their DDoS attack readiness in objective, quantitative terms.

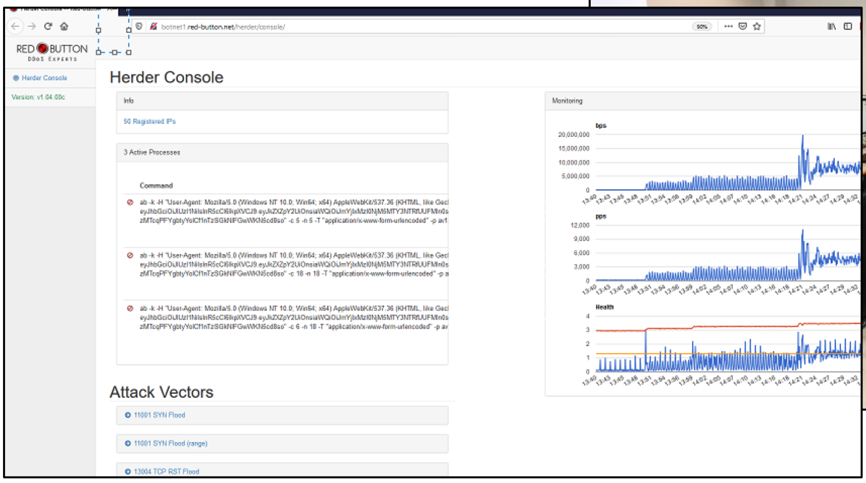
For more information about Red Button, see www.red-button.net.

For more information about the DDoS Resiliency Score (DRS) standard, please visit www.ddosresiliencyscore.org.

Our vendor-neutral advantage

Red Button is unique in its vendor-neutral approach. We truly believe that one of the key factors for organizations still suffering from DDoS is that they entrust their DDoS protection to vendor-biased sources. Such entities do not (and cannot, business-wise) disclose the limitations of their solutions. Red Button does not form liaisons with any DDoS mitigation solution provider. Thus, we remain fully committed to the customer's best interests.





botnet1.red-button.net/herder/console/

RED BUTTON DDoS EXPERTS

Herder Console

Version: v1.04.00c

Herder Console

Info

50 Registered IPs

3 Active Processes

Command

```
ab -k -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXZpY2UiOnsiaWQiOiJmYjkMzI0NjM5MTY3NTRfUUFMIn0s
zMTcqPFYgbtyYoICf1nTzSGkNIFGwWKN5cd8so" -c 5 -n 5 -T "application/x-www-form-urlencoded" -p av1.

ab -k -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXZpY2UiOnsiaWQiOiJmYjkMzI0NjM5MTY3NTRfUUFMIn0s
zMTcqPFYgbtyYoICf1nTzSGkNIFGwWKN5cd8so" -c 18 -n 18 -T "application/x-www-form-urlencoded" -p a

ab -k -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZXZpY2UiOnsiaWQiOiJmYjkMzI0NjM5MTY3NTRfUUFMIn0s
zMTcqPFYgbtyYoICf1nTzSGkNIFGwWKN5cd8so" -c 6 -n 18 -T "application/x-www-form-urlencoded" -p av
```

Attack Vectors

11001 SYN Flood

11001 SYN Flood (range)

13004 TCP RST Flood

RED BUTTON

DDoS Experts