SWORDSEC

SwordSec DDoS Simulation Testing: Comprehensive Report

Example Company

CONFIDENTIALITY & PROPRIETARY

This document contains confidential and proprietary information that must not be disclosed outside of the customer ("the Customer"), transmitted, duplicated or used for any purpose other than its intended use. Without the explicit written consent of the Customer, the information contained herein shall not be used or disclosed in whole or in part. SwordSec provides no assurance that the information contained within this document is complete or free of errors.

This report is for the exclusive information of the Customer and the Customer's management. It must not be utilized, disseminated, cited or referred to for any other intentions, nor included or cited in full or in part in any document, without our prior written authorization.

Executive Summary

Introduction: Brief overview of DDoS threats and the importance of robust protection.

Introduction to SwordSec and our expertise in cybersecurity.

Attack Vector	Layer	Target	Rate	Conclusion
UDP Flood		Router	1Gbps	PASS
SYN Flood		Website	1M PPS	PASS
ACK Flood		Website	1M PPS	PASS
ICMP Hit-and-run		Website	1M PPS	PASS
HTTPS Flood		Website	5K RPS 50K RPS	FAIL
HTTPS Flood		API (REST)	5K RPS 50K RPS	FAIL

General Information

Checklist

Takes	Owner	Status
Test Planning Meeting Meet with customer to define test content.	All	Done
Fill Out Test Plan Document Fill out this document (‘Test Plan’ section).	SwordSec	Done
Approval Customer to sign low, notify ISPs and hosting.	Customer	Done
DDOS TESTING	All Parties	Done
Summary Report	SwordSec	Done

Approvals

Company	Person	Approval Date
Customer	Mr.....	----------
Customer	Mr.....	----------
SwordSec	Mr.....	----------

Test Methodology

Methodology	Description
Simulated Attacks	Execution of diverse DDoS attacks including volumetric, protocol, and application layer in a controlled environment, ensuring no disruption to live systems.
Real-Time Monitoring	Continuous monitoring to adjust attack parameters and assess system resilience.
Data Analysis & Reporting	Post-test analysis to identify defense strengths and weaknesses with detailed reporting on findings and actionable recommendations.
Follow-Up & Continuous Improvement	A review meeting to discuss results and an ongoing testing strategy for sustained defense readiness.

Bots Location

To ensure a thorough and realistic DDoS testing environment, SwordSec conducts simulations from multiple global locations. Our tests are executed from four strategic regions to emulate a wide range of attack vectors and scenarios:
Asia, Europe, Americas, Middle East

Asset List

The following list describes the assets targeted during the test.

Name	URL/IP/Address	Description	Asset Monitoring
Organization Website	https://---------	The organization primary website	
API (REST)	https://---------	The organization API. This is the most critical resource.	
Organization router	---*----*----	The IP address of the organization router.	

ATTACK VECTORS

Test plan summary table.

Time		Attack Vector	Botnet Size	Volume	Target	Conclusion
Hour	Delta Duration					
22.00	00.00 00.00	Test Start				
22.00	00.00 00.15	UDP Flood	80	10Gbps	----------	PASS
22.15	00.20 00.05	Cool Down				
22.30	00.35 00.15	SYN Flood	80	1M PPS	----------	PASS
22.45	00.45 00.05	Cool Down				
22.30	00.35 00.15	ACK Flood	80	1M PPS	----------	PASS
22.45	00.45 00.05	Cool Down				
22.50	00.50 00.15	HTTPS Flood	80	5-50K RPS	----------	PASS
23.05	01.05 00.05	Cool Down				
23.10	01.10 00.15	HTTPS Flood	80	5-50K RPS	----------	PASS
23.25	01.25	Test End				

UDP Flood <> Organization Router

Name	UDP Flood against organization router.
Attack Vector	UDP Flood port 80
Target	--------
Volume	10Gbps
Expected Mitigation	Mitigation by ISP
Log	Time 22.16 UDP Flood Started Site down ----------
Result	Initially, the website was inaccessible. However, after six minutes, the internet service provider successfully mitigated the attack and the site was restored.

SYN Flood <> Organization Website

Name	SYN Flood against Organization website
Attack Vector	SYN Flood port 443
Target	--------
Volume	1M PPS (packets per seconds)
Expected Mitigation	Mitigation by ISP
Log	Time 22.45 SYN Flood Started Site down ----------
Result	Attack mitigated by ISP

ACK Flood <> Organization Website

Name	ACK Flood against Organization website
Attack Vector	ACK Flood port 443
Target	--------
Volume	1M PPS (packets per seconds)
Expected Mitigation	Mitigation by ISP
Log	Time 22.50 SYN Flood Started Site down ----------
Result	Attack mitigated by ISP

ICMP Hit-and-run <> Organization Website

Name	ICMP Hit and Run against Organization website
Attack Vector	ICMP Hit and Run
Target	--------
Volume	1M PPS (packets per seconds)
Expected Mitigation	Not Mitigation
Log	Time 23.00 ICMP Flood Started 23.01 Stop 23.02 23.03 Stopping the attack Site down ----------

Result	Attack mitigated by ISP

HTTPS Flood <> Organization Website

Name	HTTPS Flood against Organization website
Attack Vector	HTTPS Flood port 443
Target	--------
Volume	5,000 RPS (requests per second) and increasing up to 50,000
Expected Mitigation	ISPs are generally unable to counteract HTTPS due to the service certificate and are unable to inspect the traffic.
Log	Time 22:50 - The attack has commenced and the website is operating slowly and unresponsively. 23:00 - We have increased the size of the attack to 10,000 requests per second, causing the website's failure to respond. 23:05 - The attack has been stopped. ---------
Result	Outage. The attack was not mitigated. At the original rate of 5K RPS, the site was slow, and at a higher rate of 10K RPS, the same condition persisted.

HTTPS Flood <> Organization API

Name	HTTPS Flood against Organization API
Attack Vector	HTTPS
Target	--------
Volume	5,000 RPS (requests per second) and increasing up to 50,000
Expected Mitigation	ISPs are generally unable to counteract HTTPS due to the service certificate and are unable to inspect the traffic.
Log	Time 23:12 Attack initiated. API unresponsive. 23:25 Cessation of attack. ---------

Result	Outage. The attack was not mitigated. At the original rate of 5K RPS, the site was slow, and at a higher rate of 10K RPS, the same condition persisted.