Privia SECURITY

DoS-DDoS Testing Service

Professional Offensive Security Services

"Keep Your Business Processes Running Without Interruption!"

The information contained in this document is related to the Professional Offensive Services provided by Privia Security Information and Consulting Services and is of a general nature. All information presented in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

"The DoS/DDoS Testing Service strengthens your infrastructure's performance and reliability by testing your system under the most challenging traffic conditions."

The DoS/DDoS Testing Service measures your network's resilience by overwhelming it with simulated traffic and determines your performance limits. Today, DDoS attacks are one of the primary methods used in cyberattacks, potentially disrupting business processes and causing system outages. These tests help identify vulnerabilities in advance, allowing necessary improvements to ensure an uninterrupted service experience.

By conducting tests under heavy traffic conditions without damaging your network, the system's behavior under maximum load is analyzed. Early warning mechanisms are tested to prevent disruption of critical business processes and traffic routing and filtering solutions are reviewed. Additionally, intervention scenarios during an attack are developed as part of the service to test your infrastructure's preparedness.

With the DoS/DDoS Testing Service, not only are existing security gaps identified, but preventive strategies against future attacks are also developed. Building a strong defense against DDoS attacks is critical for business continuity and customer satisfaction.

Service Components

Traffic Simulation

In this phase, the system's limits are tested using different traffic scenarios. High traffic conditions similar to real attack situations are created to evaluate performance bottlenecks and response times. The results contribute to improving the infrastructure and developing service continuity strategies.

Capacity Measurement

This determines how much traffic the systems can handle. Errors and performance issues that may occur under increasing load conditions are assessed. The goal is to identify critical thresholds and detect necessary improvements for the network infrastructure.

Filtering Controls

The effectiveness of CDN, firewalls, load balancers and other network devices is analyzed. Traffic routing strategies are recommended to ensure service continuity and effectively isolate malicious traffic. These controls enable early detection and prevention of potential attacks.

Alert Mechanisms

The performance of monitoring and alert tools is tested to optimize response times during an attack. The speed of system responses to threats is analyzed and the accuracy of early warning mechanisms is evaluated.

Intervention and Recovery Plans

Recommendations are provided for developing intervention and recovery plans to be implemented during and after DDoS attacks. These plans ensure systems return to normal as quickly as possible, guaranteeing business continuity.

FAQ

What is a DDoS attack?

A DDoS (Distributed Denial of Service) attack is a type of attack aimed at overwhelming a system's resources to prevent it from providing services.

What is the difference between DDoS and DoS attacks?

DoS (Denial of Service) attacks originate from a single source, whereas DDoS attacks are carried out using multiple devices (botnets), making them much harder to detect and stop.

How can a DDoS attack be prevented?

DDoS attacks can be significantly mitigated using protection methods such as firewalls, CDNs, load balancers and traffic filtering.

What should be done during a DDoS attack?

As soon as the attack is detected, analyzing traffic and filtering malicious traffic are the most important steps. Contacting the service provider and notifying the security team are critical measures to mitigate the impact of the attack.

How do DDoS protection services work?

They detect abnormal traffic flows and activate filtering and blocking systems to prevent systems from being overloaded.

Which layers do DDoS attacks target?

DDoS attacks can occur at various layers of the OSI model. The most common targets are the network layer (Layer 3), transport layer (Layer 4) and application layer (Layer 7).

What is a DNS Amplification attack?

DNS Amplification is a type of attack where the attacker sends a small query and receives a large response, which is then directed to the target server. These attacks rapidly consume the system's bandwidth.

Are there free solutions for DDoS protection?

Some providers, such as AWS Shield Standard, offer basic DDoS protection for free. However, more advanced protection typically requires paid solutions.

Why are DDoS attacks dangerous for businesses?

DDoS attacks cause service interruptions and decrease customer satisfaction. In critical infrastructure sectors like finance and energy, even the smallest downtime can lead to significant financial losses.

How long do DDoS attacks last?

The duration of a DDoS attack varies. Some attacks may last only a few minutes, while others can continue for hours or even days. A strong protection infrastructure quickly mitigates the effects of these attacks and ensures minimal damage.

Your Trusted Partner in Cybersecurity

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

Global and Local Cybersecurity Solutions

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

A Secure Future Through Advanced Technology

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "Privacy For You," we bring a fresh, innovative perspective to security and privacy—

Privia
SECURITY