RAZORTHORN

DoS Testing

SERVICE BENEFITS

- ✓ **Enhanced System Resilience**: DoS testing helps identify vulnerabilities within the system, strengthening against real world DoS attacks.
- ✓ **Improved Incident Response**: Helps in developing effective strategies for a rapid response to ongoing DoS attacks.
- ✓ **Informed Investment**: Assists in guiding resource allocation towards critical systems.
- ✓ **Compliance and Trust**: Displays a solid commitment to security, improving customer and stakeholder confidence.

OVERVIEW

Denial of Service (DoS) Testing, also known as stress testing, is a critical cybersecurity assessment that evaluates the resilience of networks and systems against deliberate denial of service attacks. These attacks strategically target essential resources to overwhelm the system, disrupting its normal operations and denying services to legitimate users. DoS testing recreates these scenarios in a controlled environment to assess the effectiveness of current system defences.

This testing involves various attack strategies, including flooding the service with UDP/TCP packets and generating multiple HTTPS requests, aiming to deplete the system's resources. The focus is on monitoring how the system handles high stress conditions in terms of performance and stability. By simulating real world adversarial methods, DoS testing identifies vulnerabilities and weaknesses, enabling proactive fortification of defences. It provides a crucial means for organisations to enhance cybersecurity resilience and address potential threats before they can be exploited by malicious actors in the dynamic landscape of cyber threats.

THE RAZORTHORN APPROACH

Scope Definition
We work closely with our clients to define the scope of the test, identifying critical systems, applications and network infrastructure to be evaluated. Clear communication on the testing window, potential impact on normal operations and any specific testing constraints is established.

Threat Modelling
A comprehensive threat model is developed to understand the potential attack vectors and vulnerabilities specific to the client's environment. This involves analysing potential targets, entry points and methods adversaries might employ to disrupt services.

Test Planning
Based on the threat model, we create a customised test plan that outlines the specific DoS attack scenarios, methodologies and tools to be employed during testing. The plan includes predefined success criteria and metrics for evaluating the impact on system performance.

Simulated Attacks
Using industry leading tools and methodologies, we simulate various DoS attack scenarios, including packet flooding, resource exhaustion and application layer attacks. Different attack vectors are tested to ensure a comprehensive evaluation of the client's defences.

Monitoring and Analysis
Throughout the testing period, we closely monitor network and system behaviour, collecting data on response times, resource utilisation and system stability. Real time analysis helps us understand the effectiveness of the client's security controls in mitigating DoS attacks.

Reporting
We will generate a detailed report providing a comprehensive overview of the test, including methodologies employed, observed vulnerabilities and the impact on the client's systems. Clear, actionable recommendations are provided to enhance the client's security levels.

Razorthorn Security
4 St Johns Road
Tunbridge Wells, TN4 9NP

razorthorn.com
0800 772 0625

office@razorthorn.com