An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2212140930

NCSC Guidance

Denial of Service Attack Guidance

14th November 2024

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP:CLEAR** information may be shared without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Introduction

A Denial of Service (DoS) attack is an attempt to make a system unavailable to the intended users. Denial of service is typically accomplished by flooding the targeted machine or resource with requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. A DoS attack comes from a single system, can range in duration and may target more than one site or system at a time. An attack becomes a Distributed Denial of Service (DDoS) when it comes from multiple systems instead of just one.

Threat actors can use DoS attacks for a range of reasons including nation state attacks, extortion and notoriety. Some objectives include:

- Social or political goals (hacktivism)
- Bad publicity for an organisation (reputational damage)
- Extortion (financial)

Types of Denial of Service Attacks

There are multiple types of a Denial of Service attack, some examples are:

1. Attacks at the Application Layer

These target the application layer (Layer 7 of the OSI model[1]) with the aim to disrupt specific services or applications by exhausting their resources. Example attacks include:

- HTTP Flood[2]: Sends seemingly legitimate HTTP requests that overwhelm the server.
- Slowloris[3]: Keeps many connections open by sending partial HTTP requests and not completing them, tying up server resources.
- DNS Query Floods[4]: Target the DNS service to exhaust its processing capacity.

[1] https://www.ecma-international.org/wp-content/uploads/s020269e.pdf
[2] https://www.cloudflare.com/en-gb/learning/ddos/http-flood-ddos-attack/
[3] https://www.cloudflare.com/en-gb/learning/ddos/ddos-attack-tools/slowloris/
[4] https://www.cloudflare.com/en-gb/learning/ddos/dns-flood-ddos-attack/

2. Volume-Based Attacks (Bandwidth Attacks)

These attacks aim to overwhelm the bandwidth of the target site or network. Examples include:

- UDP Flood[5]: Overloads the target with User Datagram Protocol (UDP) packets.
- ICMP Flood: Uses Internet Control Message Protocol (ICMP) packets (e.g., ping floods[6]) to saturate the network.
- Amplification Attacks: Exploit vulnerable services to generate a large response from a small request (e.g., DNS amplification[7]).

3. Protocol Attacks

These attacks focus on exploiting weaknesses in the network protocols to consume server resources or network equipment, disrupting service. Examples include:

- SYN Flood[8]: Abuses the TCP handshake process, leaving the server with half-open connections.
- Ping of Death[9]: Sends oversized or malformed packets, causing crashes.
- Smurf Attack[10]: Utilizes ICMP packets with spoofed source IP addresses to flood the target through an amplification network.

4. Resource Depletion Attacks

These attacks target server resources such as CPU, memory, or disk space. Examples include:

- Apache Range Headers Attack[11]: A type of attack that exploits how servers process range headers in HTTP requests.
- NTP-based Attacks[12]: Exploits Network Time Protocol servers to deplete server processing power.

[5] https://www.cloudflare.com/en-gb/learning/ddos/udp-flood-ddos-attack/
[6] https://www.cloudflare.com/en-gb/learning/ddos/ping-icmp-flood-ddos-attack/
[7] https://www.cloudflare.com/en-gb/learning/ddos/dns-amplification-ddos-attack/
[8] https://www.cloudflare.com/en-gb/learning/ddos/syn-flood-ddos-attack/
[9] https://www.cloudflare.com/en-gb/learning/ddos/ping-of-death-ddos-attack/
[10] https://www.cloudflare.com/en-gb/learning/ddos/smurf-ddos-attack/
[11] https://www.rapid7.com/db/modules/auxiliary/dos/http/apache_range_dos/
[12] https://www.cloudflare.com/en-gb/learning/ddos/ntp-amplification-ddos-attack/

5. Advanced Persistent DDoS (APD)

These are long-term, continuous attacks that combine different types of DDoS methods. The goal is to exhaust the target over an extended period and force it to shut down services or scale up defenses. Examples include:

- Combination of Layer 7 (application) and volumetric attacks deployed intermittently over weeks or months.

6. Botnet-based Attacks

These attacks utilize large networks of compromised devices (botnets) to carry out coordinated and highly distributed attacks. Examples include:

- Mirai Botnet[13]: Known for infecting IoT devices and launching large-scale DDoS attacks.
- Mozi Botnet[14]: Focuses on targeting IoT devices and routers.

[13] https://www.cloudflare.com/en-gb/learning/ddos/glossary/mirai-botnet/
[14] https://malpedia.caad.fkie.fraunhofer.de/details/elf.mozi

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Preparing for Denial of Service Attacks

Understand Your Environment

Know the points in your environment which are vulnerable to a DoS attack and determine who is responsible for each. The main areas to consider are as follows:

Know Your Environment

- Network Connectivity
  - Supporting infrastructure services such as DNS and email
  - Network equipment at the public edge such as firewalls and gateways
- Computing Resources
  - Accessible websites
  - Web mail and VPN services
  - Cloud based infrastructure
- Storage
  - Application logs
  - Server storage
  - Database Capacity

Upstream Defences

Your Internet Service Provider can put certain protection controls in place.

Protection Controls

- Understand the DoS mitigations your ISP has in place for your account
- Third party DoS mitigation services
- Have a secondary service provider for critical systems

Response Plan

Plan your response to an attack so that critical services can continue during the attack.

Respond To Attack

- Have a secondary plan for essential services
- Retaining VPN or administrative access during an attack
- Have a separate means of communication in place

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

General Mitigation Strategies

Mitigation Strategies

- Maintain effective partnerships with your upstream network service provider and understand what assistance they may be able to provide during an attack
- Consider DDoS mitigation services from providers that specialise in DDoS attacks
- During an attack provide your upstream network service provider with the attacking IPs so they can implement restrictions on their end
- Enable firewall logging to determine where the DDoS may be originating
- Apply DDoS protection on edge devices
- Apply all vendor patches
- Setup an out-of-band access channel for communications during an attack

Further Reading

- https://www.cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf
- https://www.cisa.gov/sites/default/files/2024-03/understanding-and-responding-to-distributed-denial-of-service-attacks_508c.pdf
- https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection
- https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2024/gorilla_bericht.html
- https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/