

Denial-of-Service Attack

Ioana BALABAN

University “Politehnica” of Bucharest, Romania
balaban.ioana04@gmail.com

Abstract

A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy. This paper presents how DoS attacks are performed, the techniques used, the attack tools, the prevention of an attack and the some of the famous DoS attacks.

Index terms: cyberattack, cybercrime, network traffic request

References:

- [1]. What is a Denial-of-Service Attack (DoS)? - Definition from Techopedia, <https://www.techopedia.com/definition/24841/denial-of-service-attack-dos>.
- [2]. Five Most Famous DDoS Attacks and Then Some | A10 Networks, <https://www.a10networks.com/resources/articles/5-most-famous-ddos-attacks>.
- [3]. DoS (Denial of Service) Attack Tutorial: Ping of Death, DDOS, <https://www.guru99.com/ultimate-guide-to-dos-attacks.html>.
- [4]. Denial of service attack | Definition & Facts | Britannica, <https://www.britannica.com/technology/denial-of-service-attack>.
- [5]. 6 DoS attacks that made headlines | CSO Online, <https://www.csoonline.com/article/3226399/security/6-dos-attacks-that-made-headlines.html>.
- [6]. DoS attack - Wikipedia, https://en.wikipedia.org/wiki/Denial-of-service_attack.