Chapter 3
Denial-of-Service (DoS) Attack and Botnet: Network Analysis, Research Tactics, and Mitigation

Arushi Arora
Indira Gandhi Delhi Technical University for Women, India

Sumit Kumar Yadav
Indira Gandhi Delhi Technical University for Women, India

Kavita Sharma
National Institute of Technology Kurukshetra, India

ABSTRACT

This chapter describes how the consequence and hazards showcased by Denial of Service attacks have resulted in the surge of research studies, commercial software and innovative cogitations. Of the DoS attacks, the incursion of its variant DDoS can be quite severe. A botnet, on the other hand, is a group of hijacked devices that are connected by internet. These botnet servers are used to perform DDoS attacks effectively. In this chapter, the authors attempt to provide an insight into DoS attacks and botnets, focusing on their analysis and mitigation. They also propose a defense mechanism to mitigate our system from botnet DDoS attacks. This is achieved by using a through access list based configuration. The artful engineering of malware is a weapon used for online crime and the ideas behind it are profit-motivated. The last section of the chapter provides an understanding of the WannaCry Ransomware Attack which locked computers in more than 150 countries.

DOI: 10.4018/978-1-7998-5348-0.ch003

INTRODUCTION

In recent years, changes in cybercrime techniques have become more pronounced and menacing. One of the evident examples is DDoS (Distributed Denial-of-Service) Attacks, which are now appearing with a new twist, using IoT (Internet of Things) to expand their target area (Bhatt et al., 2017; Yadav et al., 2018). IoT has impacted the digital technology in a way, altering how we think or live (Dey et al., 2017). The technology promises to ease our living by providing convenience and practically improving our communication with our surroundings (Jain & Bhatnagar, 2017; Elhayatmy et al., 2018). The concept of "Anonymity of Internet" is used in the cyber attacks, changing their scale and scope. The Internet is one area where assiduousness is mandatory and security should be a priority. "The Internet is becoming the town square for the global village of tomorrow" was rightly stated by Bill Gates, co-founder of the Microsoft Corporation. The Internet provides us with a huge range of resources and services and has become a platform for numerous commercial activities like online banking, online shopping, publicity, marketing, advertising etc. (Tayal, 2017). The Internet is an open platform when compared to the current circuit-switched networks (ATMs, the analog telephone network, etc.); hence this makes it easier for attackers to enforce a cyber attack on devices connected to the Internet. The reason behind this is that the former is implemented in software using general-purpose computing hardware. Also, standardized and open technologies using servers are reachable through the Internet. Therefore, services like these suffer from internet threats just like HTTP-based services (Mukherjee et al., 2016). This chapter will focus on the Denial-of-Service attacks (Carl et al., 2006) and Botnet analysis (Alejandre et al., 2017), their detection (Park & Lee, 2001) and mitigation (Zhang et al., 2016). It has been appropriately said by Art Wittmann that, "As we've come to realize, the idea that security starts and ends with the purchase of a prepackaged firewall is simply misguided", therefore, in this chapter hybrid mitigation techniques for DoS attacks and botnets are presented (Shrivastava et al., 2010).

Man is a curious being. From the very beginning, communicating and curiosity have encouraged and led to underground research. Over these years, online financial transactions, attackers have shifted their focus from communicating to commercialization and monitory profits. Most computer systems that belong to large organizations contain valuable information about the users or business activities. The attackers are well experienced and know the methods for information retrieval, its location, and extraction for financial gain. Therefore, to protect their resources, organizations are setting up system security, staffing and defensive technologies to protect their information and computer systems (Matallah et al., 2017; Yamin & Sen, 2018). This can reduce the risk of successful attacks but it does not cure the problem completely (Kimbahune et al., 2017). Some attackers, on the other hand, are attracted to individual machines because of lack of security measures taken by the user.

The first section of the chapter explains the DoS attack types; DoS attack techniques along with its symptoms and defense techniques (Desai et al., 2016; Saha et al., 2016). The attacker of a DoS attack prevents the utilization of the resources by the user. In the attack, the bandwidth of the user is reduced and the network is flooded, thereby disrupting a service. Distributed attacks also came into existence soon after Denial of Service attacks. In Distributed attack, separate sites are used for execution to as Distributed Denial-of-Service (DDoS) attacks. The types of DoS attacks that are explained in the chapter are Denial-of-service as a service, Advanced persistent DoS (APDoS) and Distributed DoS (Mirkovic & Reiher, 2004; Feinstein et al., 2003) after which its symptoms are listed. These symptoms comprise of speed issue or slow *network performance,* unreachable websites, drastic number of spam emails or