Chapter 7

DDoS Attacks and Their Types

Dileep Kumar
Adama Science and Technology University, Ethiopia

ABSTRACT

Billions of people rely on internet to discover and share ideas with the world. However, the websites are vulnerable to deliver the attacks, preventing people to access them. The recent study of global surveys showed that DDoS Attacks evolved in strategy and tactics. A Distributed Denial of Service (DDoS) attack is a new emerging bigger threat that target organization’s business critical services such as e-commerce transactions, financial trading, email or web site access. A DDoS attack is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. To create attacks, attackers first discover vulnerable sites or hosts on the network. Then vulnerable hosts are exploited by attackers who use their vulnerability to gain access to these hosts. This chapter deals with the introduction, architecture and classification of DDoS Attacks.

INTRODUCTION

The core concepts of cyber security are Availability, Integrity, and Confidentiality. In Computing, a Denial-of-Service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. The attacker sends a large number of special requests to the server machine. When the load is too much for the server to cope up with, it will fail to respond to the requests. When a legitimate user tries to access the server, the requests will time out. In DoS attacks, the malicious packets are sent from single machine.

Today, DoS attacks are usually distributed, known as Distributed Denial of Service (DDoS) Attacks. A DDoS attack is a tactic to attack on the availability of services of a victim system or network resource launched indirectly from multiple compromised computers. Examples include

- Attempts to “flood” a network, thereby preventing legitimate network traffic
- Attempts to disrupt connections between two machines, thereby preventing access to a service
- Attempts to prevent a particular individual from accessing a service
- Attempts to disrupt service to a specific system or person

DOI: 10.4018/978-1-4666-8761-5.ch007
DDoS Attacks and Their Types

Massive Distributed Denial of Service (DDoS) attacks have the potential to severely decrease backbone availability and can virtually detach a network from the Internet. The DDoS attacks impact the availability of information resources by targeting organization’s business critical services such as ecommerce transactions, financial trading, email or web site access.

There would be multiple victims in DDoS Attacks; the owner of the targeted system, the users of the targeted system and the users of the targeted systems. A computer used in the attack is known as a bot. A group of co-opted computers is known as botnet. Although the owner of the co-opted computer typically is unaware that their computer is compromised, they are nevertheless likely to suffer degradation of service and malfunction.

It is very difficult to identify, avoid and minimize impact of DDoS attack due to its many to one configuration. The Internet design raises several security issues concerning opportunities for DDoS attacks.

- **Highly Interdependent Internet Security**: DDoS attacks are commonly launched from systems that are subverted through security-related compromises. Regardless of how well secured the victim system may be, its susceptibility to DDoS attacks depends on the state of security in the rest of the global Internet.
- **Limited Internet Resources**: Each Internet entity (host, network, service) has limited resources that can be consumed by too many users.
- **Intelligence and Resources are not collocated**: A peer-to-peer communication paradigm led to storing most of the intelligence needed for service guarantees with end hosts, limiting the amount of processing in the intermediate network so that packets could be forwarded quickly and at minimal cost. At the same time, a desire for large throughput led to the design of high bandwidth pathways in the intermediate network, while the end networks invested in only as much bandwidth as they thought they might need. Thus, malicious clients can misuse the abundant resources of the unwitting intermediate network for delivery of numerous messages to a less provisioned victim.
- **Accountability is not enforced**: IP spoofing gives attackers a powerful mechanism to escape accountability for their actions, and sometimes even the means to perpetrate attacks (reflector attacks, such as the Smurf attack).
- **Control is distributed**: Internet management is distributed, and each network is run according to local policies defined by its owners. The implications of this are many. There is no way to enforce global deployment of a particular security

In addition to the internet design issues, the following are motives ranging from political extortion to random attacks by amateurs.

- **Hactivism or ideological and political differences**: Anonymous and LulzSec are two of the most publicized notorious hacktivist groups. They have brought down the websites of the world’s largest and most prestigious brands and organizations. Often these groups send clear warning signals by openly discussing their targets, releasing their plans to news outlets and posting their intentions on social media and blogs before launching the attacks.
- **Extortion and other financial motivators**: A potential attacker will often email or call with a ransom demand, ranging from several hundred dollars to hundreds of thousands of dollars, depending on sophistication and the motives of the attacker. Paying the ransom is not good enough. Rather, have a proactive DDoS mitigation plan in place and be ready to deploy it.