A Novel Approach to Develop and Deploy Preventive Measures for Different Types of DDoS Attacks

Khundrakpam Johnson Singh, National Institute of Technology, Manipur, India
Janggunlun Haokip, National Institute of Technology Manipur, India
Usham Sanjota Chanu, NIELIT, Imphal, India

ABSTRACT

In the new era of computers, everyone relies on the internet for basic day-to-day activities to sophisticated and secret tasks. The cyber threats are increasing, not only theft and manipulation of someone’s information, but also forcing the victim to deny other requests. A DDoS (Distributed Denial of Service) attack, which is one of the serious issues in today’s cyber world needs to be detected and their advance towards the server should be blocked. In the article, the authors are focusing mainly on preventive measures of different types of DDoS attacks using multiple IPtables rules and Windows firewall advance security settings configuration, which would be feasibly free on any PC. The IPtables when appropriately selected and implemented can establish a relatively secure barrier for the system and the external environment.

KEYWORDS

DDoS Attacks, DoS Attacks, Firewall, Hping3, ICMPv6, IPtables, Netscreen, Prevention

1. INTRODUCTION

The internet has grown tremendously in a very short period of time and has become a necessity for everyone in every corners of the world. Through the Internet infrastructure, people can share their files, communicate with each other from distant places in real time and also performed tasks cooperatively from different places by contributing their computing resources. Furthermore, one can easily join the network and communicate with any other system in the network. These services also come with a lot of vulnerabilities. Attacks can take many forms, ranging from an attack on the physical IT (Information Technology) environment, overloading of network connection capacity, or through exploitation of application weaknesses (Bahaa & Al-Musawi, 2012).

Gligor et al. defined DoS (Denial of Service) as a group of authorized users of a specific service that deny service of another group or authorized users (Yu & Gligor, 1990). Here, the former group makes the specified service unavailable to the latter group for a period of time which exceeds the intended waiting time. Network components are at risk of DoS for two main reasons.

First, the resources such as bandwidth, processing power, and storage capacities of targeted servers are limited and so networks and systems can be exhausted by DoS attacks. Second,
Internet security is highly interdependent and the weakest link in the chain may be controlled by someone else who is not a legitimate user, thus taking away the ability to be self-reliant (Fu, Papatriantafilou, & Tsigas, 2012).

In DDoS attacks, attackers do not use a single system or host for their attacks but a cluster of several computers to do a coordinated attack. The evolution of solutions to resolve or prevent the occurrence of the attacks in turn promotes the evolution of the attacks itself. Nowadays DoS attacks have been evolved to DDoS attacks (Kumar & Selvakumar, 2011). DDoS attacks can be classified into three categories: First, Application-layer DDoS attacks which target windows, apache, open BSD (Berkeley Software Distribution), or other software with vulnerabilities and could crash the servers. These attacks utilized malicious packets which appear to be legitimate application layer (layer 7) requests to the server and later crash it. The layer 7 DDoS attack includes attacks on Apache HTTP (Hyper Text Transfer Protocol) Server, Microsoft IIS, and includes tools such as Slowloris (National Cybersecurity and Communications Integration Center, 2014; Occupyweb, 2015).

Second, a protocol DDoS attacks which deals with attacks on the protocol level. This category includes SYN (Synchronous flag) flood, Ping of Death, etc. These attacks often use the server's resources rather than bandwidth going to and from the server. They can also use the resources of the network equipment on the periphery of the server such as firewalls, intrusion detection systems, and switches. Smurf attacks (a type of protocol level DDoS attack) use ICMP (Internet Control Message Protocol) to broadcast a spoofed IP. Fraggle attacks are same as the Smurfs but use UDP (User Datagram Protocol). SYN floods, ping of deaths sends oversized ICMP with the same destination, source IP, port.

Third, volume-based DDoS attacks include ICMP floods, UDP floods, and other kind of flood attacks that are performed through spoofed packets. These attacks are the simplest. The attacker simply sends a large volume of packets to the target thereby using up all the target's resources like bandwidth, CPU (Central Processing Unit) and memory, etc.

There are two main reasons for people's interests in launching the DDoS attack. Firstly, there are various effective easy-to-use automatic tools available freely for attacking any victim and it does not require expertise. Secondly, it is usually impossible to locate the attacker's whereabouts without extensive human interaction or without new features in most routers of the Internet (Abhilash & Kumar, 2011; Chang, 2000).

In this paper, we divide the work into two categories. First, we generate some of the DoS/DDoS attacks and observe the exhaustion of system resources in terms of CPU and memory. Second, we provide solutions to minimize the effect of the generated attacks. We closely observe and analyze the exploitation of victim resources after deploying the prevention policy.

Here, we experimentally generate various DoS/DDoS attacks using hping3 from Kali Linux of 2 GB RAM (Random Access Memory) and 40 GB storage capacity against Ubuntu machine having 2 GB RAM and 40 GB storage. For HTTP-GET attack, we used OWASP (Open Web Application Security Project) Switchblade 4.0 attack tool. The attacks are mitigated using IPTables firewall rules implemented using Juniper Networks NetScreen-5GT. ICMPv6 Router advertisement and ICMPv6 Neighbour Solicitation attacks are performed using THC (The Hacker Choice)-IPv6 attack toolkit from Ubuntu Linux against windows machine. The ICMPv6 attacks are mitigated using windows firewall advance security settings.

The paper is organized as follows: Section 2 discusses the related work. Section 3 presents effects of different types of DDoS attacks. Section 4 presents the mitigation stage. Section 5 presents the discussion. Section 6 provides the conclusion of the paper and finally section 7 gives the direction to future works.

2. RELATED WORKS

Munivara et al. (2014) had presented a broad classification of various DDoS attacks, DDoS defensive architectures such as source-end, victim-end and intermediate architectures. They also presented
Related Content

A TPM-based Secure Multi-Cloud Storage Architecture grounded on Erasure Codes
[www.igi-global.com/article/a-tpm-based-secure-multi-cloud-storage-architecture-grounded-on-erasure-codes/171190?camid=4v1a](www.igi-global.com/article/a-tpm-based-secure-multi-cloud-storage-architecture-grounded-on-erasure-codes/171190?camid=4v1a)

Securing Online Bank’s Big Data Through Block Chain Technology: Cross-Border Transactions Security and Tracking
[www.igi-global.com/chapter/securing-online-banks-big-data-through-block-chain-technology/234813?camid=4v1a](www.igi-global.com/chapter/securing-online-banks-big-data-through-block-chain-technology/234813?camid=4v1a)
Cryptographic and Steganographic Approaches to Ensure Multimedia Information Security and Privacy
www.igi-global.com/article/cryptographic-steganographic-approaches-ensure-multimedia/37582?camid=4v1a

A New Meta-Heuristics for Intrusion Detection System Inspired from the Protection System of Social Bees
www.igi-global.com/article/a-new-meta-heuristics-for-intrusion-detection-system-inspired-from-the-protection-system-of-social-bees/171188?camid=4v1a