Chapter 12
A Survey on Denial of Service Attacks and Preclusions

Nagesh K.
Pondicherry Engineering College, Department of Computer Science and Engineering, Puducherry, India

Sumathy R.
Pondicherry Engineering College, Department of Computer Science and Engineering, Puducherry, India

Devakumar P.
Pondicherry Engineering College, Department of Computer Science and Engineering, Puducherry, India

Sathiyamurthy K.
Pondicherry Engineering College, Department of Computer Science and Engineering, Puducherry, India

ABSTRACT

Security is concerned with protecting assets. The aspects of security can be applied to any situation-defense, detection and deterrence. Network security plays important role of protecting information, hardware and software on a computer network. Denial of service (DOS) attacks causes great impacts on the internet world. These attacks attempt to disrupt legitimate user's access to services. By exploiting computer's vulnerabilities, attackers easily consume victim's resources. Many special techniques have been developed to protest against DOS attacks. Some organizations constitute several defense mechanism tools to tackle the security problems. This paper has proposed various types of attacks and solutions associated with each layers of OSI model. These attacks and solutions have different impacts on the different environment. Thus the rapid growth of new technologies may constitute still worse impacts of attacks in the future.

DOI: 10.4018/978-1-7998-5348-0.ch012

INTRODUCTION

The main objectives of network security are to attain availability, integrity, and confidentiality of computer system resources (includes hardware, software, firmware, data and telecommunications) (Kumar, 2004). Security protocol acts as an important component of network security. Ahead data communications between any network entities, security protocols is implemented for entity authentication, key agreement and secure associations formed. For example, Internet Key Exchange (IKE) protocol uses public key schemes to authenticate the protocol initiator to prevent unwanted traffics flooding (Jain, 2011). Sometimes security protocols may have DOS vulnerability, because some of the stages of verification process may involve resource consuming executions which may cause the attackers to invoke legitimate user's resources. Consequently, protocol designers should ensure about this problem and develop secure protocol to handle DOS attacks. Thus, security protocols can be used to provide confidential data and crucial service. This results in secure network connection and data communication. The components of security programs are authority, framework, assessment, planning and maintenance.

In a denial of service attack, when attacker's attack messages are initiated from multiple hosts which are distributed over the network, it is called as Distributed Denial of Service (DDOS) attack. In contrast, when offender's attack messages are originated from a single host called as Single-Source Denial of Service (SDOS) attack. A DOS attack is a depraved attempt by a single attacker or a group of attackers to cripple an online service. The cause and effects of denial-of-service attacks could even become life-threatening. A group of terrorist attacked 19,000 French websites hit by DDOS on January 7, 2015. This attacked low level government as well as business websites. Several websites of the Paris had been hacked and defaced by ISIS flag. The few symptoms of the attacks are abnormal slowdown of network performance, inadequacy of a particular site, inefficiency to access any site etc. Usually DOS attackers are inspired by different following reasons-financial/economical gain, invariably slow network performance, revenge, ideological belief, intellectual challenge, service unavailability, cyber warfare (Prasad, 2014).

This paper discusses the various DOS attacks involved in each layers of the OSI model and solutions are provided for those attacks. We have provided the best solution for these attacks and even more solution for these attacks may be invented in the future. The impacts of attacks may vary in different platform or environment such that solutions will too have certain restrictions with respect to the domains. And also, we discuss about the significant of DOS attacks that all affected some of the industries. A detailed survey of DOS attack that all experienced by many of the countries all over the world. There are many attacks emerging as technology developing in parallel. We can't able to judge the best solution for the attacks, but we can able to take preventive measures to solve the issues or problems which may occur.

DDOS FILTERING PROCESS

The Figure 1 presents the process of Distributed Denial of Service as follows:

- Initially, the hacker attempt to gather information about the targeted system;
- Next step, using any basic techniques exploits the weakness of the system;
- DDOS sensor (any related mechanisms) is used to detect and filter these attacks;
- DDOS filter (any related tools), removes the detected attacks;
- Finally, the distributed customers can utilize the network without any issues.