Simulation of DDoS Attack & Real Time Prevention Algorithm

Silica Kole, Deepak Kumar Gupta, Pulkit Goel

Abstract— A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. The term is generally used with regards to computer networks, but is not limited to this field, for example, it is also used in reference to CPU resource management. There are two general forms of DoS attacks: those that crash services and those that flood services. One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately[1].

Index Terms— DDoS , Website Attack , IP Spoofing ,DDoS Prevention , DDoS Detection.

1 INTRODUCTION

THE DDoS Attacks or Denial Of Services Attack have become very common amongst Hackers who use them as a path to fame and respect in the underground groups of the Internet. Denial of Service Attacks basically means denying valid Internet and Network users from using the services of the target network or server[2]. It basically means, launching an attack, which will temporarily make the services, offered by the Network unusable by legitimate users.

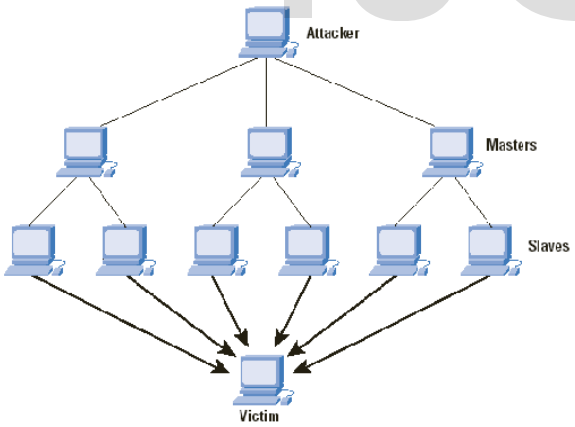

Figure 1 : General DDoS attack idea

In others words one can describe a DOS attack, saying that a DOS attack is one in which you clog up so much memory on the target system that it cannot serve legitimate users. Or you send the target system data packets, which cannot be handled by it and thus causes it to either crash, reboot or more commonly deny services to legitimate users. DOS Attacks are of the following different types :-

1. Those that exploit vulnerabilities in the TCP/IP protocols suite.
2. Those that exploit vulnerabilities in the Ipv4 implementation.
3. There are also some brute force attacks, which try to use up all resources of the target system and make the services unusable.

2 METHODOLOGY

2.1 Simulation

Taking the underlying principal, we are carrying on the simulation of DDoS Attack using some simple UNIX commands and pearl scripts.

Watch –n 0.2 "GET http://www.moviepsycho.com"

Command Name : watch

Execute a program periodically, showing output full screen watch runs command repeatedly, displaying its output (the first full screen). This allows you to watch the program output change over time.

By default, the program is run every 2 seconds; use -n or --interval to specify a different interval.

Command Name : GET GET - WWW user agent This program can be used to send requests to WWW servers and your local file system. The request content for POST and PUT methods is read from stdin. The content of the response is printed on stdout. Error messages are printed on stderr. The program returns a status value indicating the number of URLs that failed. Font and Paragraph Formatting.

- *Silica Kole is currently faculty at Bharati Vidyapeeths College of Engineering, New Delhi as Assitant Professor E-mail : silica.kole@yahoo.com*
- *Deepak Kumar Gupta is currently pursuing B.Tech in Computer Science Engineering from BVCOE, Delhi (GGSIP University) Ph: +91-9871453624 ,E-mail : deepak91g@gmail.com*
- *Pulkit Goel is currently pursuing B.Tech in Computer Science Engineering from BVCOE, Delhi (GGSIP University) Ph: +91-9910965551 E-mail : pulkitgoel.17@gmail.com*

3 PREVENTION TECHNIQUES

3.1 Detecting DDoS

In order to prevent these DDoS attack to happen first of all we need to detect a possible DDOS attack. And for efficient detection we need to keep tab on certain parameters such as

1. Memory Usage
2. CPU Usage
3. Sudden Increase In Number Of Guests Online
4. Number Of Entry Processes
5. Data coming from same IP Address

3.2 Prevention Mechanisms

There are two main mechanisms by which we can prevent DDoS Attacks

1. Limiting the Number of Different Users Accessing the Website.
2. Limiting The Frequency Of Website Access By A Particular IP Address.

4 ANALYSIS

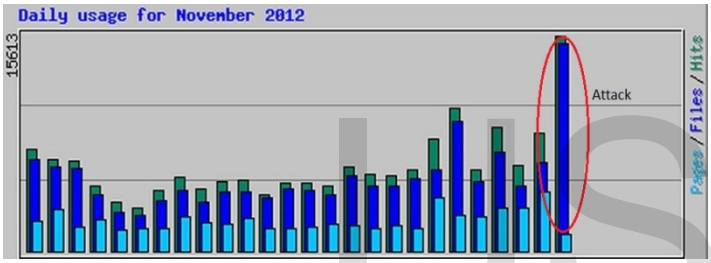

Figure 2 : DDoS Attack Detected

Figure 3 : DDoS Attack Prevented

5 SOURCE CODE

5.1 Extract of actual code for Limiting number of Users

```
if($cookie && $othercookie > 0) $itime = 20;  // Minimum number of seconds between visits
else $itime = 10; // Minimum number of seconds between visits
$ipenalty = 120; // Seconds before visitor is allowed back
if($cookie && $othercookie > 0)$imaxvisit = 100; // Maximum visits per $iteme segment
else $imaxvisit = 50; // Maximum visits per $iteme segment
$iplogdir = "./iplog/";
$iplogfile = "iplog.dat";

$ipfile = substr(md5($_SERVER["REMOTE_ADDR"]), -2);
$oldtime = 0;
if (file_exists($iplogdir.$ipfile)) $oldtime = filemtime($iplogdir.$ipfile);
$time = time();
if ($oldtime < $time) $oldtime = $time;
$newtime = $oldtime + $itime;

if ($newtime >= $time  + $itime*$imaxvisit)
{
touch($iplogdir.$ipfile, $time + $itime*($imaxvisit-1) + $ipenalty);
$oldref = $_SERVER['HTTP_REFERER'];
header("HTTP/1.0 503 Service Temporarily Unavailable");
header("Connection: close");
header("Content-Type: text/html");
echo "<html><body bgcolor=#000000 text=#00FF00 link=#ffff00>
<font face='Verdana, Arial'><p><b>
Too many page views (more than ".$imaxvisit." visits within ".$itime." seconds)
by your IP address on moviepsycho.com. Unregistered visitor hackers get less privileges.
</b>
";
echo "Please wait ".$ipenalty." seconds and try again.</p>
Or go to our facebook page <a href='https://www.facebook.com/MoviePsycho4U'></font>
</body></html>";
```

5.2 Extract of Actual Code for Limiting Packet size

```
<?php
$limit = 2;
$sql = new mysqli($host, $user, $pass, $dbname);
 $ip = $_SERVER['REMOTE_ADDR'];
 $ip = ip2long($ip);
 $date = date('Y-m-d H:i:s', strtotime('-1 minute'))
 $result = $sql->query('SELECT ID FROM `lastactivity` WHERE `IP` = '.$ip.' AND `datetime` > "'.$date.'";');

if($result && $result->num_rows)
 {
        $id = $result->fetch_array(MYSQLI_NUM);
        $sql->query('UPDATE `lastactivity` SET `datetime` = '.  date('Y-m-d H:i:s').' WHERE `ID` = '.$id[0].';');
}
else
{
      $result = $sql->query("SELECT COUNT(*) FROM `lastactivity` WHERE `datetime` > \"$date\" LIMIT $limit");
       if($result && $result->num_rows) {
       $num = $result->fetch_array(MYSQLI_NUM);
```

```
        if($limit == $num[0]) {
         echo 'sorry! already at the limit. You are not allowed
         to enter. Goodbye';
          die();        }
          Else
          {
          $sql->query('INSERT INTO `lastactivity`(`IP`,
         `datetime`) VALUES('.$ip.', '.  date('Y-m-d H:i:s').');');
            }       }
    }
```

echo 'Hi there! Welcome to this website. You\'re very lucky to get a chance of seeing this';

REFERENCES

[1] Nicholas Weaver, "*Warhol Worms: The Potential for Very Fast Internet Plagues,*" Nicholas Weaver, U.C. Berkeley BRASS group, "Potential Strategies for High Speed Active Worms: A Worst Case Analysis," February 2002

[2] David Neil ,"*Analyzing Distributed Denial Of Service Tools: The Shaft Case,*" Sven Dietrich, NASA Goddard Space Flight Center; Neil Long, Oxford University; David Dittrich, University of Washington