DISTRIBUTED DENIAL OF SERVICE TESTING METHODOLOGY

From

NETWORK INTELLIGENCE
An ISO 27001 Company

An article on Distributed-Denial-of-Service (DDoS) attacks, their various types and our methodology for testing the robustness of your network against them.
## Document Tracker

<table>
<thead>
<tr>
<th>Author</th>
<th>Version</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manasdeep</td>
<td>November 2012</td>
<td>Document Created</td>
</tr>
</tbody>
</table>
NOTICE

This document contains information which is the intellectual property of Network Intelligence. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of Network Intelligence.

Nothing in this document constitutes a guaranty, warranty, or license, expressed or implied. Network Intelligence disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non infringement of intellectual property or other rights of any third party or of Network Intelligence; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of Network Intelligence.

Network Intelligence retains the right to make changes to this document at any time without notice. Network Intelligence makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Copyright
Copyright. Network Intelligence (India) Pvt. Ltd. All rights reserved.
NII Consulting, AuditPro, Firesec, NX27K is a registered trademark of Network Intelligence India Pvt. Ltd.

Trademarks
Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.
## Contents

1. Introduction .................................................................................................................................................. 5  
2. Rationale for using DDoS attacks against banks ....................................................................................... 6  
3. Variants of DDoS attack: ............................................................................................................................. 7  
   a. ReDoS (Regular Expressions DoS Attack) ................................................................................................. 7  
   b. Billion laughs (XML Parser DDoS): ........................................................................................................... 7  
   c. Peer-to-peer DDoS attacks: ..................................................................................................................... 8  
   d. Permanent denial-of-service attacks ......................................................................................................... 8  
   e. Distributed reflected denial of service attack (DRDoS) .......................................................................... 8  
   f. Un-intentional denial of service ................................................................................................................ 9  
4. Challenges in mitigation defences against DDoS attacks ........................................................................... 10  
   a. Rapid Scaling of the attacks ..................................................................................................................... 10  
   b. Problem with peer-to-peer DDoS .............................................................................................................. 10  
   c. Distinguishing between the legitimate traffic and attack traffic .............................................................. 10  
5. Our Approach ............................................................................................................................................. 11
1. INTRODUCTION

A Distributed Denial-of-Service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users by using multiple hosts attempting to connect simultaneously to the victim machine. It generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Attackers typically target sites of high-profile web servers such as banks, credit card payment gateways, and even root name servers.

Commonly, the attack involves saturating the target machine with external requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. The objective of these DDoS attacks is to either force the targeted computer(s) to reset, or consume its resources so that it can no longer provide its intended service.

Impact
These attacks violate Internet proper use policy, the acceptable use policies of virtually all Internet service providers. They cause huge productivity losses to the organizations as the services offered by the organizations are rendered unavailable due to saturation of servers. They damage hard earned positive brand image of a financial institution by rapid erosion of its stakeholder's confidence.

What can happen due to DDoS?
- Rapid consumption of computational resources, such as bandwidth, disk space, or processor time.
- Disruption of routing information.
- Unsolicited resetting of TCP sessions.
- Disruption of physical network components in very short time interval.
- Sudden spike or maxing out of the processor's usage
- Multiple errors triggered in interconnected machines.
- Multiple errors in the sequencing of instructions, forcing the connected computer into an unstable state or lock-up.
- Almost instant resource starvation and/or thrashing in interconnected machines i.e. to using up all available facilities.
2. **RATIONALE FOR USING DDoS ATTACKS AGAINST BANKS**

Although, DDoS attacks are quite noisy and easily noticeable by both victims and banks; this works largely as a shadow attack. This is a smart diversion technique to camouflage the real hacker intention; which is to siphon out user data while security and network administrators are busy fixing congested data network pipes. DDoS outages also deflect attention from the bank wire transfers making them unable to reverse the transactions (if found). For e.g., when Sony diverted its technical efforts to subvert the DDoS attack launched by Anonymous hacker group, information of more than 100 million customers was quietly siphoned by hackers in background.

Additionally, panic waves and knee-jerk reactions are spread among public at large when customers find out that they are unable to access their accounts online. Many important transactions are simply delayed or rolled back during peak business hours.

This results in major reputation loss for financial institutes. Banks will be forced to face embarrassing litigation suits if these issues are not promptly fixed. Longer the "Access Denied" period stays, greater the financial and reputation losses along with rapid depletion of stakeholder confidence are suffered by these financial institutions.
3. Variants of DDoS Attack:

a. ReDoS (Regular Expressions DoS Attack)

The Regular expression Denial of Service (ReDoS) exploits the fact that most Regular Expression implementations may reach extreme situations that causes them to work very slowly (exponentially related to input size). An attacker can use this to consume resources and leave them hanging for a very long time.

Evil regexes are those that get stuck on crafted input and can be different depending on the regular expression matcher that is under attack.

**Necessary factors for evil regex to occur:**

- The regular expression applies repetition (“+”, “*”) to a complex sub-expression;
- For the repeated sub expression, there exists a match which is also a suffix of another valid match.
- If a regex itself is affected by a user input, the attacker can inject an Evil Regex, and make the system vulnerable.

A Regex is called "evil" if it contains regular expression:

- Grouping with repetition
- Inside the repeated group
- Repetition
- Alternation with overlapping

For e.g.:

- \((a+)\)+
- \( ([a-zA-Z]+)*\) and so on...

b. Billion laughs (XML Parser DDoS):

A billion laughs attack is a type of denial-of-service (DoS) attack which is aimed at parsers of XML documents. The attack consists of defining 10 entities, each defined as consisting of 10 of the previous entity, which expands to one billion copies of the first entity.

Example:

```xml
<?xml version="1.0"?><!DOCTYPE lolz [<ENTITY lol "lol">]<ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
<ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
<ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
<ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
<ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
```
When an XML parser loads this document, it sees that it includes one root element, "lolz", that contains the text "&lol9;". However, "&lol9;" is a defined entity that expands to a string containing ten "&lol8;" strings. Each "&lol8;" string is a defined entity that expands to ten "&lol7;" strings, and so on. After all the entity expansions have been processed, this small (< 1 KB) block of XML will actually contain $10^9 = a billion "lol"s, taking up almost 3 gigabytes of memory.

c. Peer-to-peer DDoS attacks:

In this DDoS attack, the attacker acts as a "puppet master," by instructing clients of large peer-to-peer file sharing hubs to disconnect from their network and connect directly to the victim's website instead. Subsequently, several thousand computers aggressively try to connect to a victim's website making web servers typically designed to handle a few hundred connections per second failing instantly when are overwhelmed by receiving requests from five or six thousand connections per second.

d. Permanent denial-of-service attacks

Also called phlashing; this attack damages a system so badly that it requires replacement or reinstallation of hardware. This attack exploits security flaws which allow remote administration on the management interfaces of victim’s hardware by replacing the device's firmware with a modified, corrupt, or defective firmware image. This essentially "bricks" the device, rendering it unusable until it can be repaired or replaced.

PDoS is a pure hardware attack. It can be much faster and requires fewer resources than using a botnet. Because of the potential and high probability of security exploits on Network Enabled Embedded Devices (NEEDs), this technique is getting popular.

e. Distributed reflected denial of service attack (DRDoS)

This attack sends forged requests to a very large number of computers that will reply to the requests. Using Internet Protocol address spoofing, the source address is set to that of the targeted victim, which means all the replies will go
and flood the target site. For e.g. ICMP Echo Request attacks (Smurf Attack) can be considered one form of reflected attack

f. **Un-intentional denial of service**

A situation when a website ends up denied, not due to a deliberate attack by a single individual or group of individuals, but due to a sudden enormous spike in popularity. This happens when an extremely popular website posts a prominent link to a second, less equipped site, for example, as part of a news story. The result is that large number of primary site's users – click that link in the space of a few hours, having the same effect as a DDoS attack on the target website. An attacker can intentionally post an interesting news link which redirects it to the victim's site, causing a DDoS Attack.
4. Challenges in Mitigation Defences against DDoS Attacks

a. Rapid Scaling of the attacks
   Mitigation mechanisms for DDoS are difficult to maintain because even if we rapidly block the large no of IP address from where the requests are originating, attacker will simply add more zombie computers to scale up the attack. Buying more redundant servers for extra load balancing won't be of much help as the attacker can also scale up the attack by merely adding more zombie computers.

b. Problem with peer-to-peer DDoS
   Although, peer-to-peer attacks are easy to identify with signatures, even tearing down connections takes server resources and can harm the server. This method of attack can be prevented by specifying in the peer-to-peer protocol which ports are allowed or not. If port 80 is not allowed, the possibilities for attack on websites can be very limited.

c. Distinguishing between the legitimate traffic and attack traffic
   It gets very difficult to distinguish the legitimate traffic from the bogus volume of attacker’s traffic coming from DDoS attack as many machines are simultaneously trying to connect to the target site and blocking a few of them won't help as attacker just needs to leverage the attack by adding “new” ones from the “botnet”.

   Taking down the site “offline” even for few hours proves self-defeating for any financial institution as thousands to millions of transactions remain stuck, or get rolled back causing millions dollars’ worth of business loss to banks etc. during peak trading hours.
5. Our Approach

a. Identify the target IP addresses
   We need to find what IP addresses are publically hosted on the internet.
   
   **What we need:**
   List of the IP addresses hosting critical services on internet

b. Identify the services or resources to attack
   Typically we look for services hosted such as Web/Application server, DNS servers, Email/Exchange server etc. We explore the known vulnerabilities and public exploits for various products
   
   **What we need to target:**
   Identify services which process large amount of financial transactions or provide user services. We can try to blocking access to them for legitimate users will have biggest impact for the target.

c. Identify the tools needed to overwhelm these offered services or resources to make them stop functioning
   
   **Email Systems:**
   Email bombs to send massive volume of emails to an address in an attempt to overwhelm the server where the emails for the target are hosted and managed.

   Filling up the mailboxes forces the mail servers to reject any legitimate mails arriving at the inbox and bounce back to sender address which causes valuable client follow-up and losing business opportunities.

   Through poor non-delivery notification design, a considerable proportion of mail services currently deployed throughout the Internet may be used as denial of service agents. By abusing a small number of vulnerable mail servers within large organizations with high Internet bandwidth connectivity, it is possible to cause the complete denial of service of critical e-mail services of any targeted organization. It is a simple process of abusing multiple SMTP services to cause a Distributed DoS (DDoS) that would increase the impact on the target.

   **Application and Web Servers:**
   KillApache DDOS tool enables us to crash any Apache web server. It works by stating multiple unsorted components in the header which causes an Apache server to malfunction.
In IIS, DDoS attacks can exist in IIS pool by opening many connections and make sure that the pool of victim website is over the limit so website is down with "service unavailable" message. We just need to send large no of requests to a vulnerable IIS server for successful DDoS attack.

**FTP Servers:**
Misconfigured FTP servers can allow an attacker to upload large files onto the server, thus reducing the space and bandwidth available for legitimate users.

**DNS Servers:**
Attackers can exploit unpatched or misconfigured DNS services to resolve domain names for external domains. Multiple such requests can cause the server to place subsequent legitimate resolution request on hold or drop those requests.

**Bandwidth Exhaustion:**
Internet exposed services are provided by the target’s internet service provider (ISP). These services are provided a large dedicated bandwidth to allow users of the service constant availability. In a normal scenario, a single attacker (with smaller bandwidth pipes) may not be able to fill up the bandwidth pipeline at the target. However, multiple such small sources, may be able to exhaust the dedicate bandwidth pipe available with the target. Some of the popular techniques used to cause bandwidth exhaustion are SYN Flood, SMURF attack etc.

**What we need:**
- Email addresses of important point of contacts (Sales, helpdesk, HR) and important individuals.
- Permission to run a quick scan for critical services like HTTP, FTP, DNS
- Multiple Dedicated bandwidth to send excessive traffic to exhaust bandwidth resources at the target’s internet pipeline

d. **Distribute the attack from multiple machines**
   We distribute attacks from different machines which simultaneously point to the target machine and send out thousands of requests per second blocking them effectively.

e. **Execute the attack**
   The above attacks can be executed at an amplified state using multiple attack origins.
Tools used:

Here are some of the popular tools we use for testing DDoS:

- **LOIC (Low orbit Ion Cannon)** – This performs a distributed-denial-of-service (DDoS) attack when used by multiple individuals on a target site by flooding the server with TCP packets or UDP packets with the intention of disrupting the service of a particular host.
- **HULK (Http Unbearable Load King)**, web server DDoS tool
- **Silent-DDoSer** - This Visual Basic tool offers attack types “UDP”, “SYN” and “HTTP”. Silent-DDoSer utilizes triple-DES and RC4 encryption, IPv6 capabilities, and password stealing functions.
- **Net-Weave** - It is a booter/bot and backdoor written in .NET and features USB spreading capabilities, TCP connection exhaustion flood, UDP flood, and a crude port 80 flood instantiated with a .NET Socket call.
- **DirtJumper v5.0**
- **Runescapeddoser** – Loaded with over 12,500 shells, that’s enough to destroy any home connection even through the biggest firewalls. Also has built in a Runescape name to IP fetcher. After fetching the IP simply press boot and IP’s are taken offline for 180 seconds.
- **KillApache tool** – An unknown flaw in the code for processing byte range headers allows versions 2.2.x of the Apache Web Server to be crippled from a single PC. This tool exploits this issue to launch DDoS attack.