Vulnerability of Network Traffic in Data Centers under Various kinds of Attacks

DAMBAR PUN[†1]
BATAJOO AMIT[†1] BISHNU PRASAD GAUTAM[†1]

IP network traffic is increasing vary fast as the numbers of users are growing rapidly. It is important that network administrators are aware of this phenomena and a careful monitoring of the traffic that is traversing their networks is necessary. Traffic monitoring and analysis is essential in order to more effectively troubleshoot and resolve issues when they occur, so to not bring network services to a stand still for extended periods of time. Many network tools are available to help administrators with the monitoring and analysis of network traffic. Using TCPDump and Wireshark for TCP packet analysis for normal and malicious traffic, especially SYN floods. In this research a detail study of SYN flood and DNS attack is studied.

Index Terms – Traffic Analysis, TCPDump, Wireshark, Distributed Denial of Service (DDoS), SYN Flood, Traffic Monitoring.

1. Introduction

A study shows that attacks against infrastructure are targeting significant resources across the Internet [1],[2],[3]. Similarly, malicious exploits are gaining access to web hosting servers, name servers, database servers and many other resources in data centers. Data centers are physical or virtual infrastructure used by enterprises to house computer, server and networking systems and components for the company's information technology needs, which typically involve storing, processing and serving large amounts of mission-critical data to clients in client/server architecture.

According to the forecast report, of IDC the total number of data centers around the world will peak at 8.6 million in 2017, and then begin a slow decline. Today's business world is becoming ever more reliant on the data center. With more workloads, more end-points, and a lot more data, demands around resources and efficient technologies continue to grow. The data center has become the heart of any modern organization. With virtualization and cloud computing at the helm, many are saying that it's great to be in the data center business. Although this may be the case from an infrastructure side, we can never forget that as more people move towards a type of platform – the bigger the target becomes [2].

Many data centers that rely on websites to serve customers and communicate with partners are on edge lately, alarmed by media reports of high-profile hacking incidents. The technology press tends to focus on cyber-attacks that involve the exploitation of operating system vulnerabilities. Nonetheless, different type of threat is quietly growing under the hood for example the Distributed Denial of Service (DDoS) attack. Report shows that DDoS attacks were up 75 percent in 2013.

The number of attacks is increasing, and the techniques used to attack servers are more complex. In the distributed denial-of-service (DDoS) attack often seen recently, multiple distributed nodes attack a single server concurrently. A malicious user tries to hack remote nodes by exploiting the vulnerabilities of software running on them, installs an attacking program on hijacked nodes, and keeps them waiting for an order to attack a victim server. When the malicious user sends a signal to them, they begin to attack to the same server.

Even if the rate of attack for each node is small, the attack traffic can cause serious damage at the victim server when the number of hijacked nodes is large.

There are many kinds of DDoS attacks, about 90% all DoS attacks are SYN Flood attacks. In this research we do the survey of the nature of DoS and DDoS attack. Practically, we can categorize that there are two major types of DoS attacks one of which is crashing type and the other is flooding type. We will discuss about flooding type of attack by giving the example of SYN attack. Furthermore, we highlight the recent problems arisen due to open resolver that leads to DNS amplification attacks. In fact, this became a serious issue recently in most of the DNS servers in Japan. This lead us to think and bring more compelling countermeasures. Thus, we have conducted an observational study in order to deepen our knowledge in regards to such kind of attacks. We have been conducting the observation and analysis of DNS amplification attacks which was practically experienced by authors while assessing the network management. In this paper, we begin our discussion from a simple nature of DoS attack and highlight the open resolver issue and DNS implication attack and the counter measure that we applied during the attack.

2. Issues and Objective of Research

Network administrators are often engaged in solving various kinds of attacks while their networks face the attacks from outsider. In order to safeguard the network from malicious attacks, a proper monitoring, managing and a proactive counter measure is required. However most of the organizations have faced security attacks and could not be well prepared due to lack of human resource and security staffs in the organization. This has been a challenging issue not for small organization but also

[†1] Wakkanai Hokusei Gakuen University

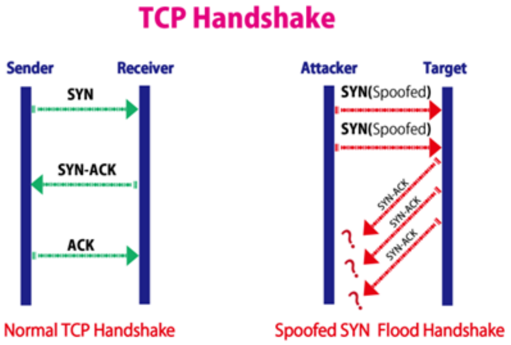


Figure 1: TCP 3-wayhandshak(1a) and SYN flood attack(1b)

for larger organization too. Our objective of this study is to provide a step wise counter measure that can be applied by the organization proactively without waiting the threats happening.

3. TCP Handshake & Nature of SYN Attack

In TCP, to establish a connection, the client sends a SYN to the server. The server allocates a buffer for the client and replies with a SYN&ACK packet. At this stage, the connection remains in the half-open state while waiting for the ACK reply from the client to complete the connection setup, after which the 3-way handshake is achieved as shown in figure (1a). TCP SYN DDoS attacks exploit the TCP 3-way handshake. Attackers send large numbers of SYN packets, with spoofed source IP addresses, to the victim servers. As a result, the SYN&ACK response packets do not reach the attackers' machines and the final ACK packets are not sent to the victim server to complete the 3-way handshake as shown in figure (1b). Therefore, resources at the victim server are tied up for these half open state connections created by the attackers preventing services to be granted to other legitimate requests. Because the packets used in SYN Flood attacks do not differ from normal TCP SYN packets except in the spoofing of the source addresses, it is difficult to distinguish them from normal TCP SYN packets at the victim server. This is why SYN Flood attacks are hard to detect.[2]

4. Case studies of DoS Attack Detection

In this section we would like to discuss the stepwise methods so that the SYN flood attack can be detected.

4.1 Detection based upon packet flow

SYN flood attack is a attack based on simple logic. It just send a large numbers of SYN packets to the victim computers where the sender does not acknowledge the reply. Instead it replicates the SYN packets with different source address. Once the the source host does not responses its ACK, then this sort of connection is called half-open-connection. This is problematic as the victim computer now remains the half-open-connections in its memory because this state is in fact a data structure which actually use some particular resources in the memory. Once this kind of half-connected sessions are increased it will eventually exhaust the victim computer and resulted in halting the system. This kind of attack has been detected since 1980s and still continues till date. In order to detect such attack, network administrator can observe the flow of packet. In this method, SYN flood attack is detected on network by careful analysis and through examination of flow statistics obtained through packet sampling. This type of method is used here to detect SYN flood attack. In order to detect such kind of packets, we set up very simple topology as shown in figure 2.

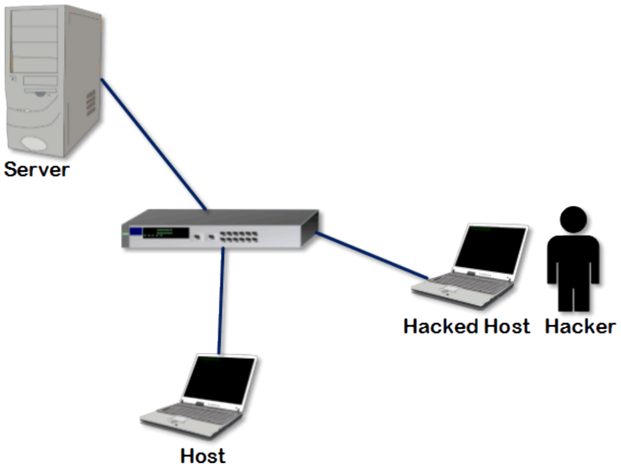


Figure 2: Experimental Network Topology for Testing Attack

We have created wired topology at our lab as shown in figure 2. We have captured 10 random sample of normal TCP packet from host pc as shown in table 1 which shows the normal pattern of the data which has been graphed in figure 1.

Table 1: Normal Packet Scenario

Normal Packets					
Type	Flags	Seq. No.	Ack. No.	Win. Size	Length
SYN	[P.]	221064898:221065106	3899984853	1026	208
SYN-ACK	[.]	208		16425	0
SYN	[P.]	208:528	1	1026	320
SYN-ACK	[.]		528	16345	0
SYN	[P.]	528:832	1	1026	304
SYN-ACK	[.]		832	16269	0
SYN	[P.]	832:1136	1	1026	304
SYN-ACK	[.]		1136	16193	0
SYN	[P.]	1136:1440	1	1026	304
SYN-ACK	[.]		1440	16117	0

Table 2: Table 2. SYN-Flood Attack with 100 threads

Case I SYN-Flood Attacks (100 Threads)					
Type	Flags	Seq. No.	Ack. No.	Win. Size	Length
SYN	[P.]	56046492:56046700	892879357	1026	208
SYN	[P.]	133297695:133298231	1021735379	16425	536
SYN	[P.]	536:576	1	16425	40
SYN-ACK	[.]		576	0	0
SYN-ACK	[.]		208	16125	0
SYN-ACK	[.]		49451205	0	0
SYN-ACK	[.]		3182055935	350	0
SYN	[P.]	3643268438:3643269898	606703307	16425	1460
SYN-ACK	[.]		1460	60	0
SYN	[P.]	1460:2920	1	16425	1460

Furthermore, we have sent 100 threads as SYN-Flood attack and captured 10 random packets as shown in table 2.

Table 3: SYN-Flood Attack with 1000 threads.

Case 2 SYN-Floods Attacks (1000 Threads)					
Type	Flags	Seq. No.	Ack. No.	Win. Size	Length
SYN	[P.]	2193432453:2193433913	1786590086	16425	1460
SYN	[P.]	1596477504:1596477632	1483634786	1026	128
SYN	[P.]	128:256	1	1026	128
SYN	[P.]	2274561012:2274562472	4049780511	16425	1460
SYN-ACK	[.]		1460	446	0
SYN	[P.]	1460:2920	1	16425	1460
SYN-ACK	[.]		2920	674	0
SYN-ACK	[.]		256	16089	0
SYN	[P.]	1460:2490	1	16425	1030

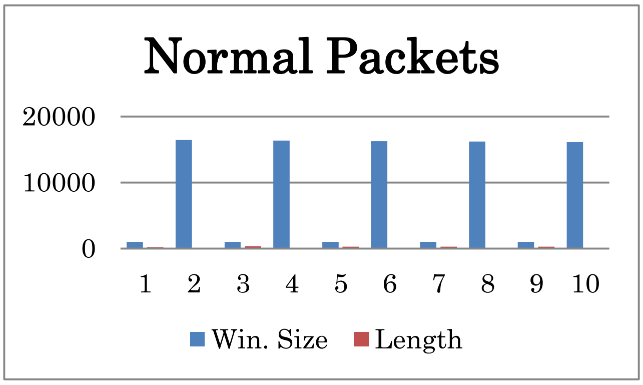


Figure 1: Packed Dumped in Normal Situation

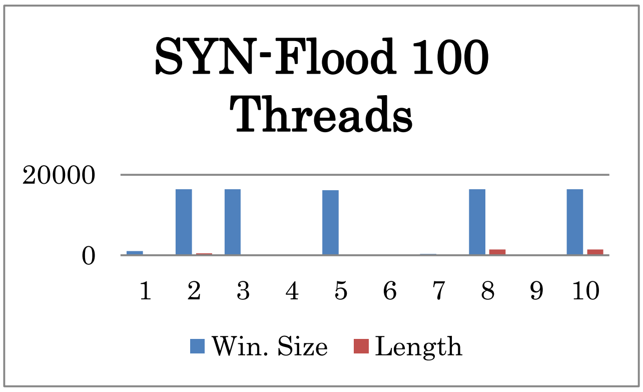


Figure 2: SYN attack with 100 Threads

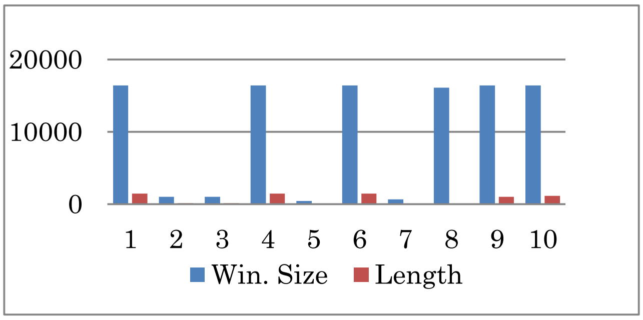


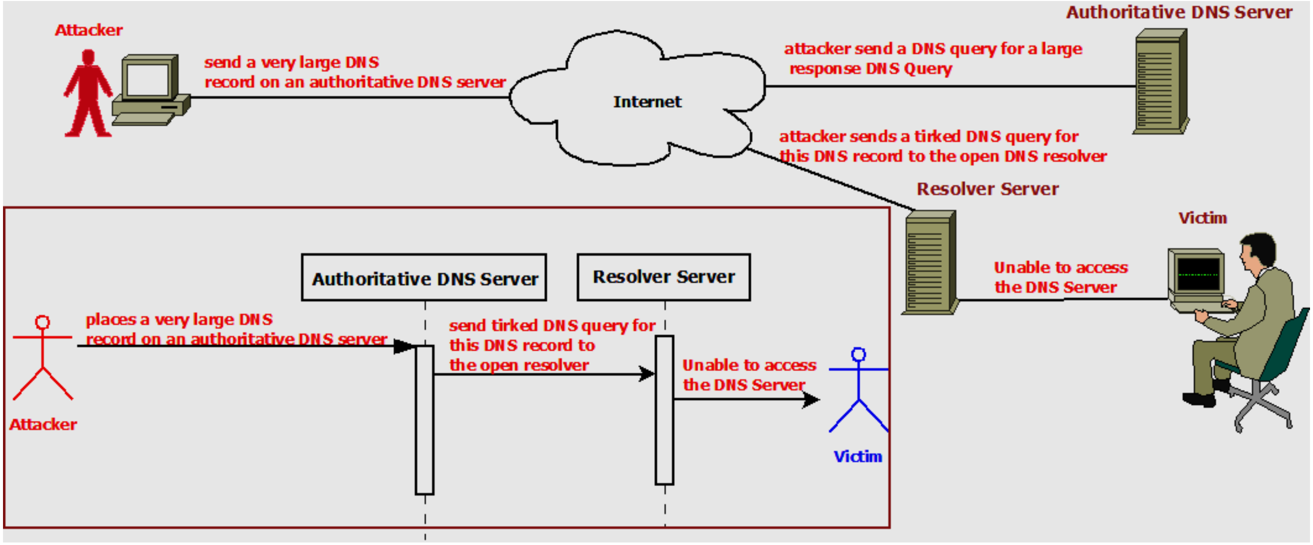
Figure 3: SYN attacks with1000 Threads

Similarly the number of threads were increased to 1000 and the data is plotted in table 3.

It has been observed that while the attacker IP is spoofed the victim server does not get ACK packet and thus it will wait for ACK and thus remained exhausted once we increase the threads more than 1000. Our observation showed abnormal pattern as shown in figure 3 and figure 4 as there is no smooth TCP handshake during the communication.

4.2 Case Study: Open resolver issues of DNS and Step Wise Counter Measure

A DNS open resolver is a state of DNS server that allows name resolving request from any IP sources [5]. These IP sources can be from within the network or outside the network regardless of its location. This kind of DNS server that performs recursive


Authoritative DNS Server
Attacker
send a very large DNS record on an authoritative DNS server
Internet
attacker send a DNS query for a large response DNS Query
attacker sends a tirked DNS query for this DNS record to the open DNS resolver
Resolver Server
Victim
Unable to access the DNS Server
Authoritative DNS Server
Resolver Server
places a very large DNS record on an authoritative DNS server
send tirked DNS query for this DNS record to the open resolver
Unable to access the DNS Server
Attacker
Victim

name Figure 4: Open Resolver and DNS Attack

Table 4: Common characteristics of open resolver

Sno	Characteristics
1	Queries are targeted for A records
2	There is no OPT resource in query
3	Most of the time sub-domain contains only characters from a-z

resolution without limiting access list is called open resolver. Particularly, a DNS open resolver is openly exposed server at which any one can query for name resolution. This kind of situation is vulnerable to malicious activities which are categorized as follows:

- Cache poisoning attacks: In this attack, attackers poisoned the cache of victim's DNS server
- Resource utilization attacks: In this attack, the attacker utilizes the resource of victim's DNS server. This will ledo consume all of the computing resource by the attacker
- DNS amplification and reflection attacks: In this attack, attacker utilize the open resolver DNS server for malicious activities which hides its own IP address but use spoofed IP address so that attacker identity is hard to determine. Furthermore, due to the spoofed source IP address, open resolver respond by sending the message to target address. In this attack, an attacker generates a large number of useless traffic inside the victim networks. These packets also travels outside of victim networks and the un-necessary DNS query floods with useless traffic.
- DNS Registrar Hijacking: By using social reengineering technique, by which attacker can use phising attack to compromise user account from vulnerable organization. This attack in malicious cases can transferred the domain name to another owner. It is thus refereed to very dangerous attack in terms of DNS attack.

Furthermore, in order to check whether the site is open resolver or not, we can check the common following characteristics however it is better to check by checking the configuration directly.

4.3 Steps of Counter Measure

4.3.1 Detect the Issue

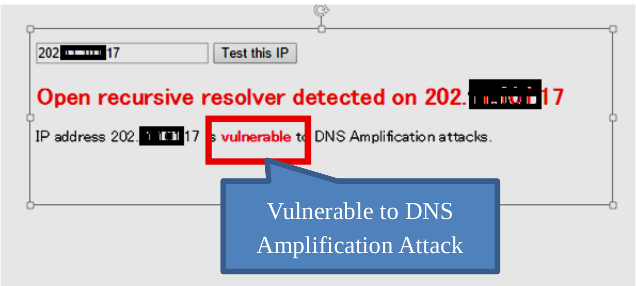
We can test whether the DNS is open resolver or not. There are open source tools that can easily test the whether the DNS of particular site is vulnerable of DNS amplification attack. In our test we found open resolver issue. Figure 3 indicates the vulnerable DNS server which was running in the victim site. IP address is hidden due to security reason.

4.3.2 Start Counter Measure

In this step, one need to check the settings of name server. As the victim DNS server was based on bind tool. Now, we need to identify a certain checkpoints which are listed below. These are done while configuring named.conf file of bind tool.

Checkpoints:

- Disable recursion: If you are enabling recursion without taking any security precaution,



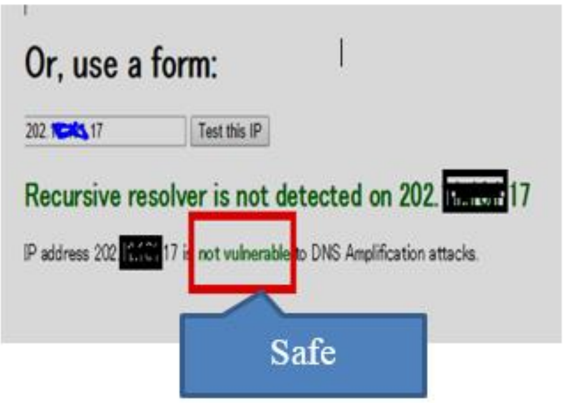
202[redacted]17 Test this IP

Open recursive resolver detected on 202.[redacted]17

IP address 202.[redacted]17 is vulnerable to DNS Amplification attacks.

Vulnerable to DNS Amplification Attack

Figure 5: Open Resolver Test



Or, use a form:

202 [redacted] 17 Test this IP

Recursive resolver is not detected on 202.[redacted]17

IP address 202[redacted]17 is not vulnerable to DNS Amplification attacks.

Figure 8: Open Resolver Test after Configuration

```
options {
        recursion no;
    };
```

- Define the trusted sources that needs recursion: First of all we need to define a variable which defines the permitable block of IP address which requires recursion this is written with acl as shown below:

```
acl "internal"{
  x/8;127.0.0.1/32;x.x.x.0/21;
};
```

- Enable recursion for trusted sources: In this step, we need to allow the recursion by including the options directive.

```
options {
 allow-recursion{internal;};
 allow-query-cache{none;};
};
```

Note that the variable internal has been used as a parameter of allow-recursion directive in the setting file.

In this way, we can resolve the open resolver DNS by restricting the resolving abilities to unwanted request.

In our practical scenario, we tested this settings with the same tool. At this time, the result was safe as shown in figure 8.

4.4 Future Works

In this study, we have shown few examples of security attacks in a network. Furthermore, we also discussed the real life experience and the stepwise counter measure faced by network administrator in the field. DNS amplification attack is well known attack which was happened recently in most of the DNS servers in Japan. Report also indicates that in 2013 and early 2014, attackers used DNS amplification in 34.9% of high volume DDoS attacks having more than 20Gbps of attack traffic and in 18.6% of all network DDoS attacks[7]. Fortunately, the counter measure is not that difficult, however, certain precautions are required while solving the problem which was well discussed in this paper.

In our future works, we will discuss more practical scenarios and the real-life attacks that the administrators are facing around the world. We will also discuss the penetration testing of the system with various examples that can benefit the network administrators.

4.5 Concluding Remarks

The major formula behind network security is to ensure security by limiting un-necessary holes from which the attackers can penetrate to the system. That means network administrator or security staff must be aware of its network and need to deny access to unauthorized hosts or users. In order to ensure high level of security, one need to utilize, firewall tool, packet filtering tool, intrusion detection system, end-users firewall, secure email and utilize secure servers. Besides applying this technique, a proactive measure of penetration testing should be utilized.

We have highlighted the major security threats based upon SYN floods followed by currently faced real working scenario by giving the example of DNS attack. It is also the fact that many organizations have not properly secured there DNS server. Open resolver DNS invites DNS amplification attack in which a attacker sends query packet to a DNS server with forged IP address. We witnessed that there are numerous kinds of attacks happened in the network. Network administrators are required to update their knowledge in order to face the dynamicity of attackers and prepare with counter measure.

Reference

1) Cisco 2014 Annual Security Report, Cisco Systems Inc. URL: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pd, Accessed: 2015/7/30

2) Data center and DDoS: ttp://www.datacenterknowledge.com/archives/2014/12/18/the-continued-threat-of-ddos-attacks-four-ways-to-address-the-concern/

3) DDoS Attack: Detecting Distributed Denial-of-Service Attacks by analyzing TCP SYN packets statistically

4) Classification of DoS Detection: Review of SYN-Flooding attack detection mechanism.

5) SSAC Advisory SAC008 DNS Distributed Denial of Service (DDoS) Attacks, A Report from the ICANN Security and Stability Advisory Committee (SSAC) March 2006

6) Douglas C. MacFarland1 , Craig A. Shue1 , and Andrew J. Kalafut: Characterizing Optimal DNS Amplification Attacks and Effective Mitigation

7) Incapsula, Inc.: 2013-2014 ddos threat landscape report. http://www.imperva.com/docs/RPT_2013-2014_ddos_threat_landscape.pdf (April 2014)