ALTEN CALSOFTLABS
AN ALTEN GROUP COMPANY

Innovate, Integrate, Transform

Denial of Service Attack

Why We Should be Aware???

www.altencalsoftlabs.com

Why We Should be Aware???

Few days back, an online post became viral saying that: "The BBC website is down because of some technical issue". Later it was discovered that a group of hackers did a DDoS attack on their server. It was shocking that such a big organization like BBC has not yet put appropriate security to avoid such cyber-attacks. Unless there is a reason for them to be concerned with security, they didn't upgrade their security. But unfortunately, they got a reason to be secure enough, but it was little late.

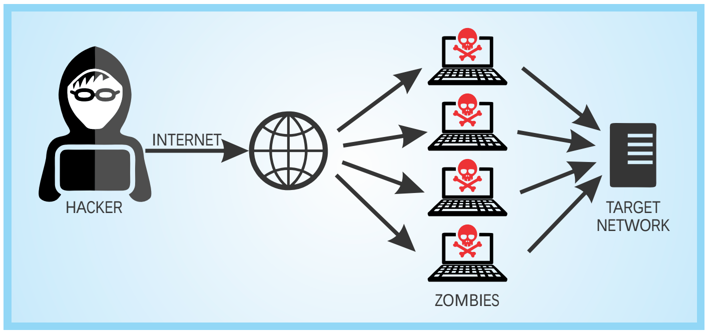
What is Denial of Service Attacks?

Whenever you find your favorite site down, it is likely that the site is under a Denial of Service attack. The more popular and the more heavily it relies on being online always, the more chances it might be under a Denial of Service attack.

In a DDoS attack, the attacker floods the target system with more requests than the system can handle. By doing this, the resource provided by the target system becomes unavailable to its users. Regular traffic on the system will get affected, either slowed down or completely interrupted.

But when a DDoS attack comes from more than one source at the same time, then this is a Distributed Denial of Service attack. This is an attack which is done using thousands (potentially hundreds of thousands) of unsuspecting zombie machines. In a DDoS attack, the attackers first infect various machines using malicious software, so that the attacker can remotely control them. These machines are then collectively known as "botnets". After gaining control over these machines, the attacker uses these machines to do a DDoS attack on a target machine. According to research, "tens of millions of computers are likely to be infected with botnet programs worldwide".

The cyber criminals use these attacks to extort money from companies by blackmailing them with the threat that they will affect their websites. These companies rely heavily on their websites for business and they can't afford their sites to be inaccessible to their users. Hence, become the big victims in these attacks.



But there are also cases in which a rival company paid these criminals to cripple the websites of their competitors. In addition, sometimes the cyber criminals combine DDoS attack with sending phishing e-mails directly to customers to a fake emergency site instead where they ask customers for their login details or in some cases their bank account details. The users mostly unaware that they are moving towards a trap, provide their confidential details to these attackers.

Statistically, in Akamai's Q1 2016 State of the internet - Security Report, the content delivery network (CDN) found out that "each year there is 125 percent increase in the denial of service attacks".

But wait. There's more. There is also an increase in attack duration. In the first quarter of 2015, the average attack duration was 15 hours, now it has increased to over 16 hours. There is a need to be concerned.

So, to fully understand the denial of service attacks, first let's look up at the types of denial of service attacks:

Types of DDoS Attack

DDoS attacks can be broadly classified into three types:

» Volume Based Attacks

This includes UDP floods, ICMP floods, and other spoofed packet floods. In this attack, the attacker's goal is to saturate the bandwidth of the attacked system.

» Protocol Attacks

This includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. In this type of attack actual server resources or those of intermediate communication equipment, such as firewalls and load balancers are consumed.

» Application Layer Attacks

This Includes low-and-slow attacks, GET/POST floods, attacks that target operating system vulnerabilities and more. These attacks comprise of seemingly legitimate and innocent requests, but the goal is to crash the web server.

The denial of service attacks are not new, there are many cases in history where such attacks have caused a great deal of loss to companies. But, some of them are unknown because the organizations have hidden the report by calling it as a technical issue to escape from the embarrassment of facing the questions of how careless they were with IT security. Let's look up at some of these incidents.

Case Studies

HSBC U.K. Banking System Taken Offline

“In January 2016 Europe’s largest financial lender HSBC suffered a DDoS attack, keeping several banking customers unable to access their accounts. The attack took place on Friday, 29th of January, and services were restored on 30th of January.

The attack was particularly damaging due to its timing. HSBC was attacked on the last Friday in January, a particularly busy day for banks as the end of the fiscal year approaches. Millions of customers - both online and mobile app users - were affected by the attack.”

Source: https://blog.surfwatchlabs.com/2016/05/04/cyber-attacks-against-banks-making-huge-impact-in-2016/

Hong Kong's Democracy Movement Flustered

“ A grassroots moment located in Hong Kong wanted to bring destruction to the Chinese government back in June 2014. This movement is called Occupy Central. They organized one of the biggest and most famous DDoS attacks in history.

Occupy Central used this DDoS attack against the Chinese government because they wanted a one man one vote system when electing officials to represent political office. At the time, the government didn't allow for such a voting system.
This all led Occupy Central to push their DDoS attack forward and brought down a major political website.”

Source: http://www.cyberdefensehub.com/famous-ddos-attacks/

The Largest DDOS Attack in History!

“Back on December 31st, 2015, on New Year's Eve a hacker group, calling themselves 'the New World Hacking' took responsibility for this huge DDoS attack. They were capable of disrupting BBC's global website, along with Donald Trump's website as well.

BBC's sites including the iPlayer, which is an on-demand service was taken down through the DDoS attack for at least three hours or more. BBC reported that the lack of response from their service was because of technical issues. However, these were no technical issues, but the well-crafted and highly organized work coming from the hands of the New World Hacking group.”

Source: http://www.csoonline.com/article/3020292/cyber-attacks-espionage/ddos-attack-on-bbc-may-have-been-biggest-in-history.html

Launch a DDOS Attack

Yes, we can launch a simple dos attack without any fancy hardware and software. All we need is the knowledge of how the denial of service attack works.

As we have seen that SYN flood is a type of Protocol based DDoS attack. In this, the attacker starts flooding the target system with syn packets. The targeted system is unable to handle this amount of TCP traffic and will stop responding after some time. This happens because whenever the target system receives an syn packet, the target system will create a TCP session to identify this session. In the normal scenario, the number of sessions created are equal to the number of actual session requests.

But, in the DDoS scenario, the attacker will flood the system with syn packets, the vulnerable system will recognize these as genuine session requests and hence will create a session for each syn packet received. The result is an unexpected number of sessions creation in less than one second which will keep on increasing until the target system is unable to create any more sessions. Even if there is a firewall to protect the system, it will be helpless because a traditional firewall only blocks traffic on the basis of IP address and port etc, but in this case, the attacker will use spoofed IP address to protect its identity. Imagine facing a tank with a book as your shield, you are certainly going to get a hit.

We can launch a simple dos attack by using a Linux tool known as hping3.

According to the main page of hping3: “Hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. Hping3 handle fragmentation, arbitrary packets body and size and can be used in order transfer files encapsulated under supported protocols.“

Dos using hping3 with spoofed IP address

To attack a target system, you need to know the IP address of the target system or the URL. After this to attack the system, just run a single line command shown below on any Linux machine:

```
hping3 -S -p 80 --flood --rand-source <address of the target system>
```

The syntax is explained below:

Hping3F	It is the name of the tool
-S	This option will set hping to send syn packets only
-p 80	The port to attack is set as 80
--flood	Send the traffic as fast as possible
--rand-source	Randomize source IP address
<address of the target system>	The target system to attack

Launching a simple dos attack on any system is not a difficult task and launching a sophisticated denial of service attack is even easier. The dark web will provide all the information on the tools and the procedure to do a denial of service attack and save yourself from getting caught as well.

Everything is not Lost Yet!

It is true that Denial of service attack is a threat to any system and can cause severe damage if not handled properly but, the fact that we have a prior knowledge of how Denial of Service attack works can give us an idea of how to mitigate the problem.

Let's take the above example in which we try to launch a simple denial of service attack as an example of how we can stop this attack.

What we tried to do as shown in the above example, we started flooding the target system with syn packets from spoofed IP address. The obvious solution to this problem is to keep a count of the number of syn packets received in a period (in seconds mostly). Depending on the deployment of the system, the number of syn packets that can be received in a particular time says 1s can be estimated. Not every system receives that many TCP sessions request in 1s. So, a limit can be set and if any more syn packets are received, we can categorize it as a denial of service attack on the system and we can start dropping the packets so that the system can be saved from a syn flood attack.

This is the process which a modern security system with the intelligence of IDS/IPS takes to identify a dos attack and protect the system. So, replacing your traditional firewall which is inadequate to handle current sophisticated attacks with a modern firewall which has a support for IDS/IPS can solve the entire problem. Not only the denial of service attacks, other sophisticated attacks can also be protected from if we use an advanced firewall.

One such example of an advanced firewall can be found at the following link:
http://www.altencalsoftlabs.com/solutions/networking-and-telecom/vfirewall-framework/

CONCLUSION

The same age old question comes again into the spotlight that whether we are going to compromise our system security at the cost of other features. A system which is insecure, but has all the features is of no use in the modern world.

Consider an example of Google, the de-facto search engine, millions of searches happen each second from users across the globe. When people are doing the browsing through Google, they have the confidence that the result will be delivered to them within seconds. But not all the traffic which is coming to Google are legitimate. Hacker groups are constantly trying to break into their servers through different attacks including the denial of service attack. Google has advanced level security in place to mitigate these attacks.

So, nowadays all the important organizations are moving towards security first approach. This trend will prove beneficial for everyone because, in the future, the level of attacks are going to increase more and more, and only if we are concerned about the security in the first place, we will be able to fight them.