DDOS ATTACKS AND NETWORK AVAILABILITY

[1]Gagandeep Kaur, [2]Jaswinder Singh

[1]M.Tech Research Scholar, [2]Assistant Professor
Department of Computer Engineering,
Punjabi University, Patiala.

Abstract : Network Continuity is one of the most crucial part in today's industry. Almost all the businesses around the world are using internet in one or other way. Availability of the network related applications are important as only authorized people can have access to those application at any time. DDoS attack is used to disrupt the availability of the business applications running over the internet. Over the time, applications related with cloud and IoT are increasing and more and more devices are connecting with the internet. These DDoS attacks are not only use for disruption of service availability, but also to steal data through the backdoor. These attacks are difficult to mitigate and is a big challenge to the organizations running web applications or Internet of Things. This paper includes various penetration testing tools for DDoS which can be used to make DDoS attacks. It also has some case studies included which shows some of the DDoS attacks made in recent years at large scale.

***Index Terms* - DDoS, TCP SYN Flood, ICMP Flood, Availability, Confidentiality, HTTP Flood.**

I. Introduction

Security has three major goals that every organization want to achieve i.e. Confidentiality, Integrity and Availability(CIA). They all are tightly integrated with each other. Confidentiality means that data going through the communication channel[3][5] between the server and the client or from one site to another site have to be secure with some encryption. Integrity means that data received from one end to other end should be in correct form and no alteration is done. Availability[1] means that the authorized users should be able to access data whenever they want to access. These days, Internet has become an important part of every industry. Almost every industry uses web in some manner, like organizations have websites, Enterprise Resource Planning(ERPs), Social Network Channels etc. These companies make large amount to money over the internet and have dedicated teams working on their internet applications or social marketing. To them, CIA is very important. DDoS[1][2] attacks can be used to disrupt the network and web services of the target. DDoS attacks are not new, the first noticeable DDoS attack occurred in 1999 and the target was University of Minnesota. It disrupts 227 systems and shuts down the server for many days. After a year, websites of companies like CNN, eBay and Amazon[14] were also attacked in similar manner. In year 2010, attacks grew at the rate of 22,000 times of average bandwidth of an internet user. Then DDoS attacks become political and also hit financial companies like Paypal,Visa and Mastercard etc. Today, DDoS attacks are mainly used for availability disruption of organization's network and web related services. Disruption of Services[4] due to some DDoS(Distributed Denial of Service attack) can be very harmful for the company as their services can be stopped which can hit them both financially and socially. For example, companies like Amazon make all their money via their E-Commerce sites and AWS Cloud Services, both these services uses Internet to get to the Clients, if any of these services got disrupted by hackers using some kind of DDoS attack, then it can decline their image and also hit them financially as well. DDoS attack is used by hackers with the use of botnets to stop the legitimate users from accessing the network and system resources of the target. Figure showing DDoS attack is shown below:

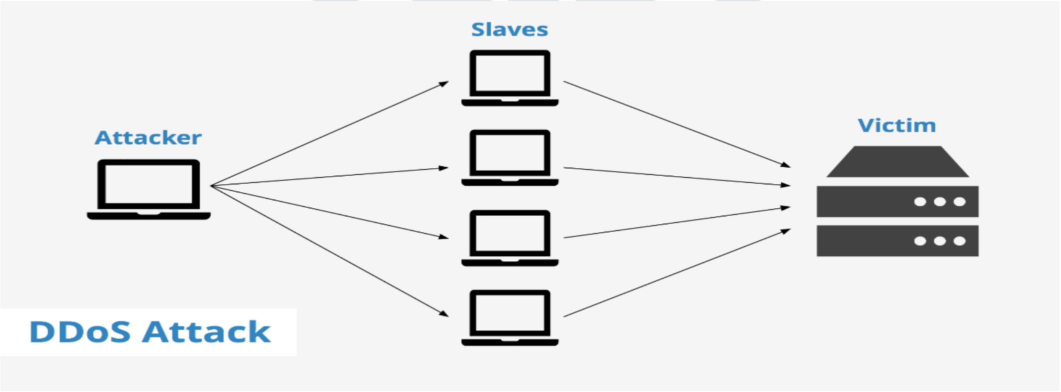

Figure 1.1 – DDoS attack

There are mostly two methods for DDoS attack. First methods uses the design vulnerabilities present in the network. Hackers send some demo packets to the target machine to confuse the application which is running on the machine. Other method uses flooding to exhaust the target machine's bandwidth or system resources. Major targets of hackers are Routers, Firewalls, Workstations, target's operating system, and applications.

II. DDoS Attacks

DDoS attacks are difficult to detect as they may seem as genuine packets and also as they are coming via botnet, therefore its very difficult to detect the attacker. Due to these difficulty in detection of the attacker and attack, it is mostly used by attackers to disrupt the network infrastructures of the organizations. Peak Attack Sizes have increased to 1.7tbps in year 2018. Below figure shows the peak attack sizes from year 2007 to 2018:

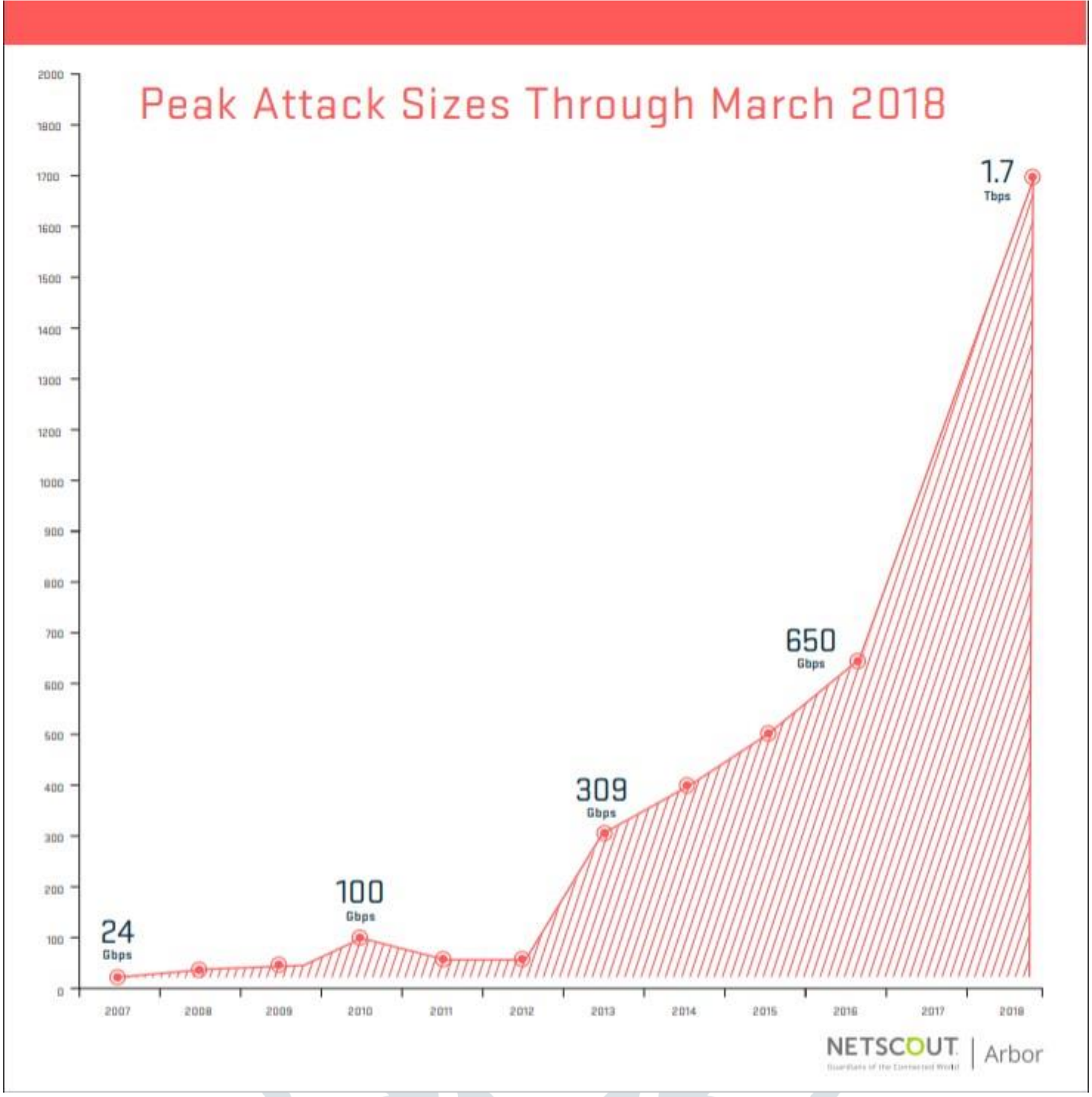

Figure 2.1 – Peak DDoS Attack Sizes from 2007-2018[18]

DDoS can also be used as a distraction by the attackers while they have a different motive, they may want companies to get confused that it is a DDoS attack to disrupt the network resources, but the target is tricked by hackers to steal the data from their data centers. Some of the recent DDoS attacks are defined in below table:

Organization Compromised	**Year**	**Description**
Arbor Networks Unnamed Client	2018	Just after few days of 1.35tbps Github attack, a massive 1.7tbps attack was measured by Arbor Networks[18] via its DDoS threat system on one of its client. This attack happened due to thousands of misconfigured memcached servers which were explosed to public internet. An request contains few bytes was sent to the exposed vulnerable servers and it triggers tens of thousands of times sized response against the target.
Github	2018	An attack of 1.35 terabits per second was clocked on Github[18], which is one of the largest ever DDoS attacks. Traffic coming via attack was monitored to be coming from over a thousand Autonomous Systems. Github was never ready for this type of attack and there were service disruptions and Github goes offline.
DreamHost	2017	A DDoS attack at one of the largest web hosting provider company and domain name registrar dreamhost[20] knocks out its infrastructure offline. Affected services includes the hosting servers, email servers and virtual private servers.
Dyn	2016	Due to emergence of Cloud and IoT, botnet is becoming more powerful and hackers get the bigger playground to play with. Mirai Botnet, which is one of the largest botnet ever, was created with the help of routers and Security Cameras. Weak security on these devices make them easy pickings for the hackers. Average IoT devices are attacked every two minutes by the hackers. Some of the major

		targets of Mirai Botnet was cloud related services like DNS provider Dyn. This, along with millons of MongoDB databases which were hosted in the cloud. According to Symantec, average organizations use around 900 cloud based applications, while their CIOs think they are using around 30, which leads to large scale of inconsistency and underestimated level of risk. Attack on Dyn[15][17], also affects large scale companies like Paypal, Netflix and Spotify.
Talk Talk	2015	A small ISP from London named “Talk Talk” is attacked by the hackers. Hackers performed a DDoS[7][8] attack on Talk Talk and suddenly their web services are disrupted and the accessibility of their website is disrupted. All the Talk Talk network team went on to troubleshooting the DDoS attack and put their all focus on resolving that issue while attackers get entry through the backdoor link and steals the customer records from Talk Talk Data Center.

III. DDoS Attack Types

There are three major types of DDoS attacks :

- **Application Layer DDoS attack:** These are the attacks[6] which target Softwares like Apache, Windows IIS, or other software vulnerabilities to generate an attack and disrupt the services.
- **Protocol DDoS attack:** These types of attacks[11] are made at the protocol level. It includes TCP SYN Flood, Ping of Death etc.
- **Volume Based DDoS attack:** This type of attack uses ICMP Floods, UDP Floods, etc via spoofed packets.

IV. DDoS Attack Methods

UDP Flood - It is a DDoS attack that targets with the help of UDP packet flooding. It attacks by flooding on random pots on a remote host. This makes host repeatedly checks for the application running on that ports and then reply with the Destination Unreachable message. This type of attacks can be made on applications using UDP like Video Conferencing Services and conference application can be disrupted using UDP Flood attack.

ICMP (Ping) Flood - It is pretty much similar to UDP Flood attacks, it creates a ICMP Request flood and send it to the target machine. This type of attack mainly utilize both outgoing and incoming bandwidth, therefore they are mainly performed using botnets. This type of attack can work on almost all the applications to choke the bandwidth of the network resources.

SYN Flood - In TCP SYN Flood attack, attacker sends SYN Floods[9][10] to the target machine and target machine replies back with the SYN-ACK and needs a TCP ACK in return from the attacking machine, but attacker never sends that back which results in target machine stucks in waiting state for all the TCP 3-Way Handshakes. It can be used to choke down applications running TCP based applications.

Ping of Death - In Ping-of-Death attack, attacker sends flood of malicious pings to the target machine. Attacker sends maximum sized IP packets to the target and it is split over multiple fragments and on the target end, he has to reassemble all the packets and when the target ends up with reassembling of packets, it ends up with packet size larger than 65535 bytes(maximum packet size) and slowly overflow memory buffers are allocated to the packet resulting in DoS attack.

HTTP Flood - In HTTP Flood attack, hacker exploits the target by sending HTTP GET or POST requests to web server or web application. This attack requires less amount of bandwidth than other attacks. Target Machine can be choked by sending hundreds of requests or by sending lots of Post messages which can disrupt the services of the web application or web site by choking the bandwidth. Some of the most commonly used DDoS attack methods and its prevention countermeasures are listed below in a table:

Table 1 – DDoS Attack and Prevention Method

Attack Method	**Prevention Method**
UDP Flood	Get a bigger bandwidth to handle peak load or large number of requests. Use a cloud based firewall which detects and drops the UDP flood.
ICMP Flood	Block ICMP by using Cloudbased Firewall which is placed before the server.
SYN Flood	Rate Limit the Traffic from a single source
Ping of Death	Block Ping Echo Requests by using Cloudbased Firewall which is placed before the server.
HTTP Flood	Place a cloud based or hardware firewall which inspects the traffic and with stateful packet inspection,

V. DDoS Attacking Tools

Below are the DDoS attacking tools which can be used to make DDoS attacks using UDP, TCP or HTTP attacks

Tool Name	Attack Types	OS	Description
LOIC	UDP/TCP/HTTP Floods	Linux, Windows	It is one of the most famous DoS attacking tool and is freely available over the internet. Hacking groups like Anonymous uses this tool. This tool performs attacks by sending UDP, TCP, or HTTP floods to the victim server.
XOIC	TCP/UDP/ICMP/HTTP Floods	Linux	XOIC comes with an easy to use GUI. XOIC comes with three different attacking modes i.e. Test Mode, Normal Mode and third one comes with TCP, UDP, ICMP, HTTP request messages.
OWASP DOS HTTP POST	HTTP Floods	Linux	It is also a very good tool to perform DDoS attack. It can be used to attack using HTTP requests.
DAVOSET	HTTP	Linux	Davoset is another freeware to perform DDoS attacks. It is a command line tools and perform DDoS on websites via Abuse of Functionality and XML External Entities vulnerabilities present on other sites.
ToR's Hammer	HTTP	Linux	It is written in Python and has some extra advantages like it can run over ToR network which helpshim to be anonymous. It is used to disrupt Apache and IIS Servers.
R-U-Dead-Yet, or RUDY	HTTP	Linux	It is a DoS tool for HTTP Flooding. It perform HTTP attack via POST method. It also has an interactive console menu.
HULK or HTTP Unbearable Load King	HTTP	Linux	This DoS attack tool can be used to create unique and obscure traffic, it can also bypass the cache engine.
Slowloris	HTTP	Linux	This tool is used for DDoS attacks. This tool send authorized traffic to the server and do not disturb other services and ports on the network targeted. It is used to hold the connection for long time. With server having false opened connections, it can overflow the connection limit and then deny the actual true HTTP connections.
HPing	TCP, UDP,ICMP, SYN	Linux	It is also used for DDoS attack by generating large number of TCP, UDP, SYN or HTTP packets.

CONCLUSION

DDoS attacks are rising every year and with the emergence of cloud and IoT, number of devices have also increased at a rapid pace. Most of the devices connecting with the internet are insecure and are used by hackers to create a botnet to perform a DDoS attack which is used to disrupt the services of targets. DDoS attacks are of three different types i.e. Application, Protocol and Volume Based. Objective of every method is same i.e. to disrupt the availability of the network infrastructure and web services of the company. Various number if tools are freely available over the internet to perform DDoS attacks. With number of insecure devices increasing at a frisk pace, DDoS attacks can only rise with the time and service providers, IoT users and companies having internet based applications find it tough to face these DDoS mayhem.

REFERENCES

[1] Nipa Patani and Rajan Patel(2017),” A Mechanism for Prevention of Flooding based DDoS Attack”. International Journal of Computational Intelligence Research.

[2] A. Shanley, M. J. "Selection of Penetration Testing Methodoligies: A Comparison and Evaluation". Australian Information Security Management Conference, 2015.

[3] Tulika Shubh and Shweta Sharma(2016),” Man-In-The-Middle-Attack Prevention Using HTTPS and SSL”. International Journal of Computer Science and Mobile Computing.

[4] Singh, H., Jangra, S., & Verma, P. K. "Penetration Testing: Analyzing the Security of the Network by Hacker’s Mind". International Journal of Latest Technology in Engineering, Management and Appplied Science , Volume V (Issue V), May-2016, pp 56-60.

[5] Ritesh Kumar Yadav(2015),” MAN IN MIDDLE ATTACK IN SSL AND HTTPS”. International Journal of Computer Science and Mobile Computing.

[6] Hakem Beitollahi and Geert Deconinck(2012), “Tackling Application-layer DDoS Attacks”, International Conference on Ambient Systems, Networks and Technologies (ANT-2012).

[7] Jai Narayan Goel, B. M. "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology". 3rd International Conference on Recent Trends in Computing 2015(Elsevier). Procedia Computer Science 57, 2015, pp 710-715.

[8] Matthew Denis, C. Z. "Penetration testing: Concepts, attack methods, and defense strategies". Long Island Systems, Applications and Technology Conference (LISAT). Farmingdale, NY, USA: IEEE, 2016.

[9] Reddy, M. R., & Yalla, P. "Mathematical Analysis of Penetration Testing and Vulnerability Countermeasures". 2nd IEEE International Conference on Engineering and Technology. Coimbatore, TN, India.: IEEE, March-2016.

[10] Shaukat, K., Faisal, A., Masood, R., Usman, A., & Shaukat, U. "Security Quality Assurance through Penetration Testing". IEEE,2016.

[11] Shivayogimath, C. N. "An Overview of Network Penetration Testing". International Journal of Research in Engineering and Technology , 3 (7), July-2014, pp 408-413.

[12] Burp Suite Editions and Features. (n.d.). Retrieved from Google: https://portswigger.net/burp

[13] D. Braue, Attack on Australian Census Site Didn’t Register on Global DDoS Sensors, Aug. 11, 2016. (http://www.cso.com.au/article/604910/attack-australian-census-site)

[14] DDoS Attacks Net, Recent DDoS Attacks, Oct. 21, 2016.(https://www.ddosattacks.net/twitter-amazon-other-top-websites-shut-in-cyber-attack/)

[15] Cisco Security Technical Report(2016)

[16] Checkpoint Security Research Report(2014)

[17]Symantec Security Report(2017)

[18] Tom Bienkowski, “No Sooner Did the Ink Dry: 1.7Tbps DDoS Attack Makes History” ,Netscout Arbor, Mar, 2018.(https://www.netscout.com/blog/security-17tbps-ddos-attack-makes-history)

[19] Real Time DDoS Attacks, “Digital Attack Map”, (http://www.digitalattackmap.com).

[20] Iain Thomson, “DreamHost smashed in DDoS attack: Who's to blame? Take a guess”, (https://www.theregister.co.uk/2017/08/24/dreamhost_massive_ddos/)