DDoS attack and email bombing using botnets

Mehul Gaur
School of Computer Science and Engineering
Galgotias University
Grater Noida
,India,gaurmehul2001@gmai.com

Saurabh Chaudhary
School of Computer Science and Engineering
Galgotias University
Grater Noida ,India
saurabh.chaudhary1906@gmail.com

Shivesh Singh
School of Computer Science and Engineering
Galgotias University
Grater Noida ,India
shiveshsingh94152gmail.com

Abstract —
Distributed Denial Service (DDoS) attacks are threats to the Internet that deplete network bandwidth or eliminate victim resources. Investigators have introduced a variety of defensive measures (such as prevention, retrieval, response, detection, and behavior) against DDoS attacks, but such attacks are growing year on year, and appropriate solutions to the problem have not yet been found. In the past, a variety of sign-based methods and unconventional methods of detecting DDoS attacks have been introduced, but only a few of them have focused on this type of disorder. Most detection methods do not provide real-time detection with high detection rate and low faux pas. In this paper, a section on finding ways to combat DDoS attacks has been introduced with the aim of understanding the DDoS problem of beginners in this research area. Visual cues are defined as their plus and minus. In addition, this review paper lists the various active classes where discovery is available. Finally, a comparison of signature-based, non-sign-based methods and hybrid detection methods is shown in tabular form..

I . INTRODUCTION

Botnets use control and control channels (C&C). Botnets use different protocols such as IRC and HTTP to start attacks. It is a challenge to detect and prevent botnet attacks due to the command and control channel. In this project we create a process to perform DDoS attacks and email explosions using the botnet process. This method does not require any prior knowledge of bots or commands and control servers. In the future, the bot sniffer monitor can be used as a browser plugin, and can help detect all web-based bots. Another launch would be to install a bot sniffer on the router. By using a bot sniffer indicator, botnet attacks can be detected and steps taken to prevent such attacks.With the help of a laptop, we will get more accurate data than data collected and recorded.

DDoS attacks occur when multiple integrated devices are used to implement one or more targeted attack. The main purpose of DdoS isto eliminate processing and networking purposes aimed at preventing official user access to services provides by the computer platfoms, thereby resulting in partial as well as complete unavailability. because of size of the face and the unity that causes this kind of attack, are very Powerful and explosive. The Scientific Community predicts that the Disruptive forces of DDOS attack , their Experience and impact Volume means to Increase at a very high voume, becomes the most serious threat to new and emerging internet service. These type of attacks come in different forms such like peak-level or lough-level attacks or a Mixture of both.

DDOS attacks can implicated as a kind of sunami because the impact of these attacks are miraclulous. DDOS attacks are massive constant problem to todays Business and can cause great Business Problems, Customer strife, and lawsuits. Without much Research and industrial work efforts DDOS Protection policy, DDOS attack have become major Problem. Increase in proportions, severity, as well as variation of attack sumbols add the severity of main Problem. The studies have developed many strategies to combat DDoS strikes on a variety of networks places.

The Contribution of Research paper is quadruple. First we can provides DDOS details

Features attack and who is behind every kind of these attacks. Secondly, we must check the most famous or recent process available to know about DDOS attacks. In Third Step, we can analyze and Evaluating one by one discovery and we can predict the detail and finally, Providing most reliable Source Relates the process of detecting DDoS attacks as a paper from a recommended magazine

LITERATURE REVIEWS

Shared Denial (DDOS) attacks have been discussed extensively in the field of computer security, mainly due to the harmful effects on the organization's employees. How ever, faces challenges under the growth of Internet users Traffic and we can say lightning speed of computer network . In the Research paper, we Present Systematic feedback of the literature or an examination of the attack of DDOS, including: a- DDOS Definition; b- types of DDOS attacks; c- various kind of DDOS acquisition strategies; d- various types of DDOS attack Predict strategies. In addition, this Research paper Provides an In-Depth Analysis of advantages as well as disadvantages of Exist DDOS acquisition assumptions to assisting the two academic and Industrialization Researcher in making a good DDOS vision as well as predictor product.

In response, we thorough examined select study and to be Identifies the precious and continous discussed DDOS attack. Different types of DDOS attacks indicate that Conduct the Taxonomy of diffenent attack. Our main Work is different types DDOS attacks, there for most of the common foms that attacker mainly use like as flood Attack and weakend attacks.

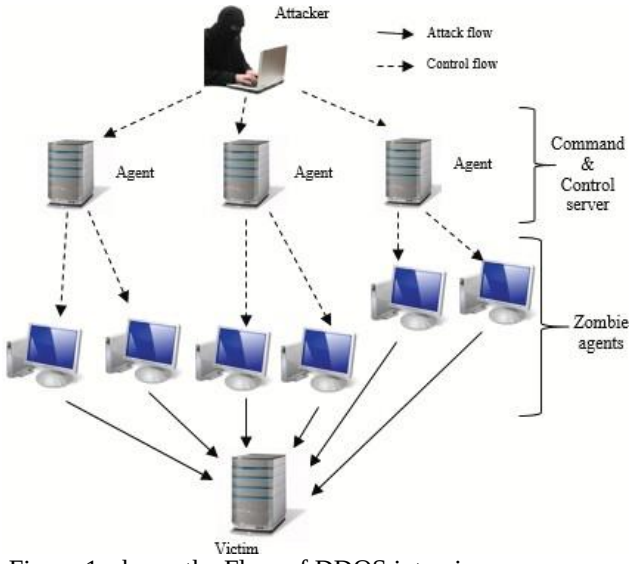

Figure 1 shows the Flow of DDOS intrusion.

		Attack type	
Network / Transport level DDoS based flooding attacks	Flooding Attacks	Spoofed/non-spoofed UDP, ICMP, DNS and VoIP	
	Protocol exploitation flooding attacks	PUSH ACK, TCP SYN-ACK, TCP SYN, ACK & RST/FIN	
	Reflection-based flooding attacks	ICMP echo request, Smurf and Fraggle attacks	
	Amplification-based flooding attacks	DNS amplification attack	
Application level DDoS flooding Attacks	Reflection / amplification based flooding attacks	VoIP flooding	
	HTTP flooding attacks	Session flooding attacks	
		Request flooding attacks	
		Asymmetric attacks	Multiple HTTP get / post flood
			Faulty Application
		Slow request / response attacks	Slowloris attack
			HTTP fragmentation attack
			Slowpost attack
			Slowreading attack

Figure--- above shows DDOS intrusion taxonomies

network based flood / transport floods require DNS rule or packetss, which aims elimination of Victim's network Band-width as well as interrupt official clients communications. Unused or unencrypted upd, icmp or dns can require other method Known as law enforcement floods that take usage of certain commands to install or use a harmfull target protocol code that uses the target app. For Ex, Tcp syn flood attacks, Tcp syn-ack flood attacks, are in this kind of attack. Some attackers take exposure-attacks build on send harmfull applications such like an Icmp Echo to moderators, Those indicators sends responses to targetes Systems by the corrupt Ip Addresss as well as by terminating the target server service. Process of flood aggression that has escalated into power is similar to an attack based demonstration. In a potential intrusion an Striker network implemented in the attackers may interact with the application or network protocol vulnerabilities existing on the Server as well as Routers. These kind of intrusion often exploits a clients who is negligent in compiling or updating systematic reviews and taxonomy of DDOS attacks Software. At the implemented intrusion package encounters an installation app, it triggers a restart, overloaded stored data usage normal System suspension. These Few examples of serious attacks as nep-tune, ping-of-death, Tcp Synn as well as Tagas39.

BOTNET DETECTION

here are many ways by which a DDoS attack can be detected. The detection of a DDoS attack can be categorised into several methods which are network mobility, machine learning, filtering method and router performance. Their main focus areas are software define networking, backbone web traffic, computer computing and big data strategies. The first job is to filter the source Ip address for all the traffic comming and leaving from your IP address. This strategy can save us from the spoof IP addresses created by attackers. By this method, it is assumed that address of the attack source is corrupted because hacker use to hide the actual source of the attack. So by checking the actual source, botnets can be detected easily.

Some other data specialists used the theory of entropy and divergence matrix to detect the attacks done by botnets. This method is used to differentiate between Flash event and DDoS attack. In this method, the process is to incoperate materices a network flow and detects that whether the network flow get affected or not, by checking the values from matrices.

Another technique was used by Perakovic el al in 2016. In that technique, we use a neural implant network and according to that, we analise the effect by applying different parameters. This method can be used to prevent us from the spoof IP addresses created by attackers. By this method, it is assumed that address of the attack source is corrupted because hacker use to hide the actual source of the attack. So by checking the actual source, botnets can be detected easily.

Another methods use map between the hop counts and the IP address, to defint the spoils IP packets from the legal ones. The reason behind this technique id mapping that made in their work. Few Authors focus main on the performance of Router. suggest maximum-minimum fair Server with Centric Router Throttles. The method control Network mess congestions with the help of the limit with a reduced or redesigned package that exceeds the Limits. The Throttle method was very functional with eliminating as well as losing congestion or traffic attackers and accepting legal passing jam, meanwhile it can also reduce the problem of overcrowding and continue to operate despite being attacked by DDoS. It shows that this approach is appropriate in the context of defeating an violent striker.

Few of the Re-searchers resolve issues on the routers themselves, the issue of congestion. suggest 2 strategies. 1st is , Local based jam Control. The method contains a Identify algo required for compounding that causes Jam. Also, It had a manage algo which reduces output of these integration with appropriate stage. The benefits is acc approach could describe in 2 categories. 1st, by asking it is

mounting Router so to create a measurement limit to support the way it works so that it can focus more on filtering incoming traffic that shows a clear attack signal. Second, it also reduces packet bandwidth usage by dropping a vicious river. This method is called pushback.
Others use the advanced process in retrospect by adding something new to there process.. The Idea's that you are taking Source Info in place of of getting an Ip Address to identfies the main address by addition of a packet tagging process. However, that' a good opportunity to win a fraudulent Ip Address apart from there is problem that the packet may leave the routes unmarked. Mr Wang propose to reduce DDOS with the help of Pushback and Resources regulation, which shows their thinking for implement a shared security strategy btw Router as well as Server victims. The approach has Improves the protection of server resources by addition of new laws so to protect Servers resources from used by strikers. They can also Increased security of Routers using a compact algorithm to protect Band-Width at the time of an intrusion.

OBJECTIVE

In this project we have shown you how hackers perform a d-dos
attack and email bombing attack live and how to take precautions
on top of these types of attacks using some basic tools of kali linux
OS
First we discussed the type of attack as
as follows: -
1. Attack of D-Dos
2. Email bombing
And then we'll show you how to do the Dos attack again
Email Bombing Successful
• Then protection from these attacks
1. IDS (Access System)
2. IPS (Access Protection System)
And then we will teach you how to make your own honey pot
using Basic Linux commands that include TWO types of Modules
1. Fast Auto Configuration
2. Manual configuration
And then show the proper function of the honeycombs
And show the good and the bad between the two
Ways

REQUIRED TOOLS

For this project we have used linux kernel which is used in several
cybersecurity projects. This project requires a little bit prior
knowledge of some linux commands.
- Wireshark
- Pentmenu (ddos file downloaded)
- An wireless network adapter
- Email bombing tool (also downloaded for git reprosetory)
- Spamsec
- Ifconfig
- And commands like cd(change directory)
chmod +x(to execute a specific file)
- Iptraf (tool used to visualize the traffic)

ACKNOWLEDGMENT

SPECIAL due to OUR PROJECT GUIDE (PRIYANKA SHUKLA MA'AM) AND REVIEWER (……) for his or her skilled INSIGHTS AND steering THROUGHOUT THE CAPSTONE method .IT WOULDN'T BE potential to finish THIS PROJECT while not THE LEADERSHIP OF OUR MENTOR AND REVIEWER.

REFERENCES—

• 1. Gray Hat Hacking **the moral** Hackers Handbook, 3rd Edition" by Allen Harper and Shon Harris.
•" **the way to** Unblock Everything on the Internet" by M.s Ankita Fadia.
• Adam J. Aviv, Andreas Haeberlen. Challenges in Experimenting with Botnet Detection Systems.2019.
• March 2013 Intelligence Report. Symantec. Cloud.
• Paul Bacher, Thorsten Holz, Markus Kotter, Georg Wicherski. Know your Enemy: Tracking Botnets. Technical
Report, The Honeynet Project. Aug 2012.
• Ethical hacking course from udemy and internshalla (2020)