International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Detecting & Isolating Anonymous Nodes Using Honeypot In Networks

Sabari Giri Murugan S*1, Ganesan T2, Thiyagu S3
*1CSE/IT, Jain University, Bangalore, Karnataka, India
2CSE, KL University, Vijayawada, Andhrapradesh, India
3CSE/IT, Jain University, Bangalore, Karnataka, India

ABSTRACT

Detecting the anonymous nodes in network by using different approaches like honey pot to measure the security of the system and detect, deflect and counteract attempts at unauthorized use of information systems.However it provides a way to detect the malicious activities in network as well as by using honey pot we can easily detect and strengthen the systems by taking mitigation strategies. Furthermore using different tools to create an DOS and DDOS attack in network and analyzing its behavior and trying to detect and mitigate those kinds of attacks with can't disrupts the resources so that the genuine users are unable to access the service. Nowadays attacks are more in real life due to the loopholes which are found in software and hardware that human is using and the information is more reliable and invaluable things, by this project we can able to learn and mitigate those loop holes by using different technologies.

Keywords : Distributed Denial of Service, Attack, Honey pot, Loop holes

I. INTRODUCTION

In today's rapid paced world continuous uninterrupted efficient service is the foundation for all service organizations. The success of any new or existing venture is critically dependent on reliability and continuous availability of service.

Progressively each individual is fetching more and more dependent on the web for resourceful and well-timed fulfilment of his need. This raises the bar for excellence too high for the service delivery organizations. They need to be extra vigilant while hardening their security road and rail network. Different kinds of threats and attacks are endlessly trying to violate their security constitution. One of the most difficult attacks to prevent is the Distributed Denial of Services (DDoS) Attack since it has direct effect on the service availability to an end user.

Honeypot and Its Types

In computer terminology, a Honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a Honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked. This is similar to police sting operations, colloquially known as "baiting," a suspect.

Based on deployment, honeypots may be classified as:

1. Production Honeypots
2. Research Honeypots

Production Honeypots: These are easy to use, capture only limited information, and are used primarily by companies or corporations. Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots do.

Research honeypots: It will run together information about the motives and tactics of the Black hat community targeting different networks. These honeypots do not add direct value to a specific organization, instead, they are used to research the threats organizations face and to learn how to better protect against those threats. Research honeypots are complex to deploy and maintain, capture extensive information, and used primarily by research, military, or government organizations.

Denial of Services Attack: In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, disrupting trade. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail and activism can motivate these attacks.

Distributed Denial of Service Attack

A distributed denial-of-service (DDoS) is a DoS attack where the perpetrator uses more than one unique IP address, often thousands of them. Since the incoming traffic flooding the victim originates from many different sources, it is impossible to stop the attack simply by using ingress filtering. It also makes it very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin. As an alternative or augmentation of a DDoS, attacks may involve forging of IP sender addresses (IP address spoofing) further complicating identifying and defeating the attack.

Mitigation Strategies: DDoS mitigation is a set of techniques or tools for resisting or mitigating the impact of distributed denial-of-service (DDoS) attacks on networks attached to the Internet by protecting the target and relay networks. DDoS attacks are a constant threat to businesses and organizations by threatening service performance or to shut down a website entirely, even for a short time. The first things to do in DDoS mitigation are to identify normal conditions for network traffic by defining ―traffic patterns‖, which is necessary for threat detection and alerting. DDoS mitigation also requires identifying incoming traffic to separate human traffic from human-like bots and hijacked web browsers. The process is done by comparing signatures and examining different attributes of the traffic, including IP addresses cookie variations, HTTP headers, and JavaScript footprints. One technique is to pass network traffic addressed to a potential target network through high-capacity networks with "traffic scrubbing" filters.

Manual DDoS mitigation is no longer recommended due to DDoS attackers being able to circumvent

DDoS mitigation software that is activated manually.[3] Best practices for DDoS mitigation include having both anti-DDoS technology and anti-DDoS emergency response services such as Arbor Networks, Incapsula, Allot, Akamai, CloudFlare or Radware. DDoS mitigation is also available through cloud-based providers.

II. METHODS AND MATERIAL

Detecting and isolating anonymous nodes using honey pot in networks, In computer terminology, a honey pot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

1. Honeypot Configuration
2. Port Scanning
3. Performing Attacks
4. Detecting Attacks

Steps:

- ✓ Monitor the network activities
- ✓ To identify the Loopholes/Vulnerabilities of the system
- ✓ Identifying the Open ports by doing scanning
- ✓ Installation & configuration of Honey pot
- ✓ Deploying Honeypots on the physical machine
- ✓ Monitoring the attacks like DOS and DDOS on the selected ports
- ✓ Finally, Honey pot able to detect the malicious activities on the system or network.

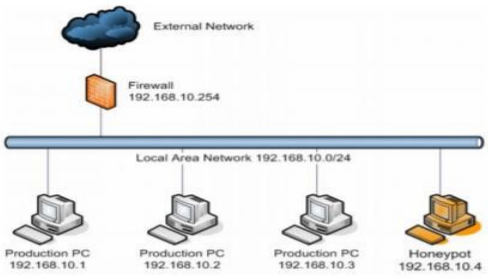

Figure 1, System Design

Pent Box 1.8: Pent Box is a security suite that can be used in penetration testing engagements to perform variety of activities. Specifically the activities include from cracking hashes, DNS enumeration and stress testing to HTTP directory brute force. Pent Box is a framework that has been written in ruby and offers some good tools that a penetration tester can use in engagement. Of course, there are better and more complex tools that can perform these activities but Pent Box offers the flexibility that contains many tools and it is very easy to use. For this reason Pent Box suite is recommended for less experienced users.

Pent Menu: Pent Menu is a bash script that is inspired by Pent Box. Designed to be a simple way to implement various network penetration testing functions, including network attacks, using wherever possible readily available software installed in most Linux distributions without having to resort to multiple specialist tools. Using Pent Menu is also very easy. We just have to download the script, make it executable and then run it. Since it is very easy to use, it is recommended for users with less experience.

LOIC: LOIC ("Low Orbit Ion Cannon") is an application developed by 4Chan-affiliated hackers designed to—when used en masse by thousands of anonymous users—launch Distributed Denial of Service (DDoS) attacks on websites like visa.com and mastercard.com, for instance. The idea behind LOIC is that it can allow you to participate in attacks even if you have no clue how to hack. Just download a copy of LOIC (available for Windows, Mac, and Linux), punch in the target information like a URL or an IP address.

III. RESULTS AND DISCUSSION

Honeypot configuration & Detection:

Step 1: Installation and configuration of Kali Linux.

Step 2: Open the command prompt terminal.

Step 3: Type —ifconfig and press enter to see the IP Configuration of the machine.

Step 4: Download Pentbox-1.8 and then extract it.

Step 5: Open the pent box folder using command terminal.

Step 6: Now open the Pent box software through the command to see the Pent Menu

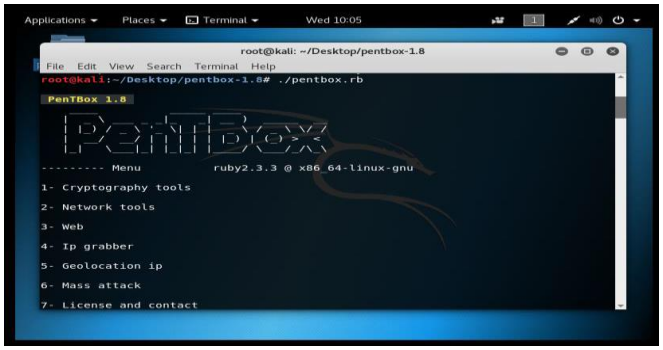

Figure 2, Pent Menu

Step 7: Open the Network tools.

Step 8: Now choose Honeypot option.

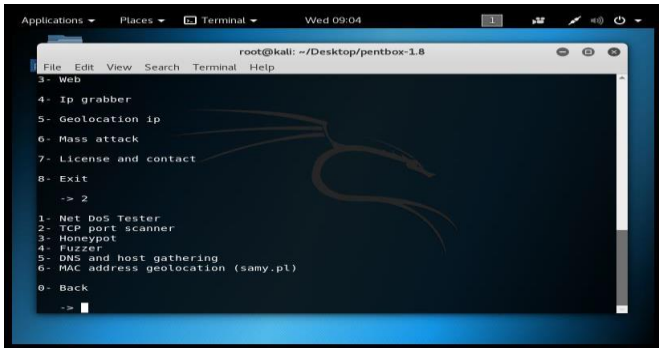

Figure 3, Network Tools

Step 10: Now select on which port the honey pot has to be deployed

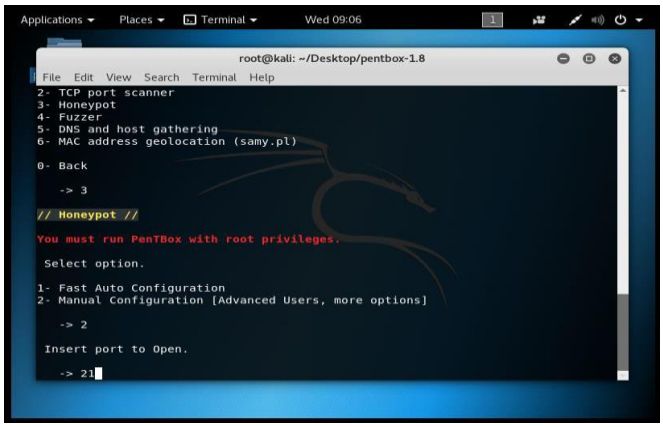

Figure 4, Honey Pot Deployment

Step 11: Select the FTP port that is port number 21 and enter the false message to show when the honey pot catches the attacker trying to open the specified port.

Step 12: Now press —y to save the log with intrusions.

Step 13: Now confirm the Log file name. Now press —y to activate beep sound when intrusion is detected.

Step 14: The honey pot is activated on port number 21 that is FTP(Control) port.

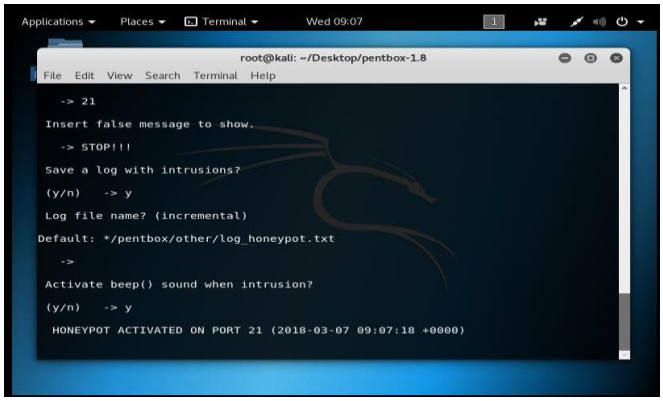

Figure 5, Honey Pot Port Activation

Step 15: Now we can able to detect the attack by using honey pot in the activated ports.

Step 16: Likewise we can deploy the honey pot in SMTP 25, SSH 22, HTTP 80 Ports to detect the malicious behavior.

DDoS Attack Detection and Implementation

Step 1: Open command Prompt.

Step 2: Ping the website.

Step 3: Create a batch file so that it doesn't display commands.

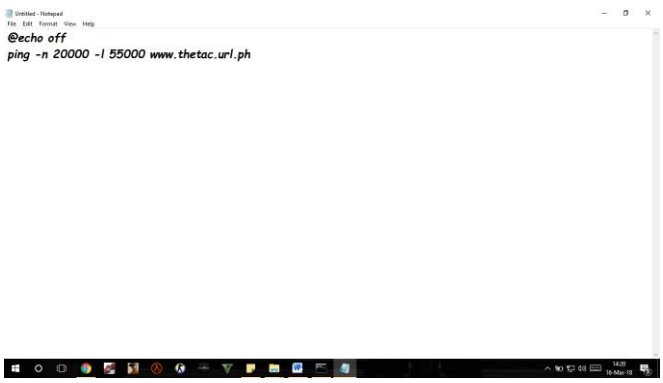

Figure 6, Creating an Batch file -Ping Flooding

Step 4: Execute the batch file multiple times to attack.

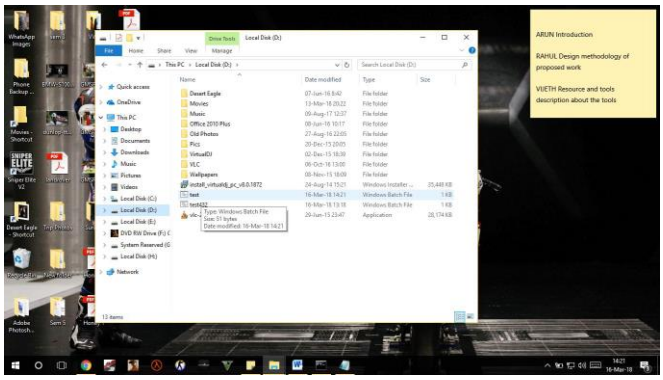

Figure 7, Execute the batch file multiple times

Step 5: Open the website and reload the page to see the deprivation of service.

IV. CONCLUSION

Distributed denial of service (DDoS) attacks are dangerous and can potentially render the production site unusable either by flooding the server network with thousands of malicious requests or crashing the server by exploiting the vulnerabilities in its software. We have successfully detected the anonymous nodes in network by using different approaches like honey pot to measure the security of the system and detect, deflect and counteract attempts at unauthorized use of information systems. Our approach provides a way to detect the malicious activities in network as well as by using honey pot we can easily detect and strengthen the systems by taking mitigation strategies. Using different tools to create a DOS and DDOS attack in network, analysing its behaviour, and trying to detect and mitigate those kinds of attacks, which can disrupts the resources so that the genuine users are unable to access the service

V. FUTURE SCOPE

In this paper, we covered an overview of the DDoS problem, available DDoS attack tools, defense challenges and principles, and a classification of available DDoS prevention mechanisms. This provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention mechanisms for fighting against DDoS threat. Software Defined Networking (SDN) is progressively replacing traditional networking. It is a new promising approach to designing, building and managing networks. In comparison with traditional routed networks, SDN enables programmable and dynamic networks. Although it promises more flexible network management, one should be aware of current and upcoming security threats accompanied with its deployment. Our goal is to analyse SDN accompanied with Open Flow protocol from the perspective of Distributed Denial of Service attacks (DDoS). In this paper, we outline our research questions related to an analysis of current and new possibilities of realization, detection and mitigation of DDoS attacks in this environment.

VI. REFERENCES

[1]. Christos Douligeris and AikateriniMitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art", Computer Networks: The Int. Journal of Computer and Telecommunications Networking, vol. 44, no. 5, Apr. 2004, pp. 643–666.

[2]. Kumar Shridhar and Nikhil Gautam, "A Prevention of DDos Attacks in Cloud Using Honeypot ", International Journal of Science and Research, Volume 3 Issue 11, November 2014, pp. 2378-2383

[3]. Aamir, M. and Arif, M., "Study and performance evaluation on recent DDoS trends of attack & defense", International Journal of Information Technology and Computer Science, 2013, pp. 54–65.

[4]. Mokube Iyatiti and Adams Michele,- Honeypots: concepts, approaches, and challenges‖, In the proceedings of the 45th annual southeast regional conference (ACM-SE), New York, USA, On Pages(s): 321 – 326, 2007

[5]. Vinu V. Das, "Honeypot Scheme for Distributed Denial-of-Service", Proceedings of the 2009 International Conference on

Advanced Computer Control, January 2009, pp. 497-501

[6]. Yu Adachi and Yoshihiro Oyama, "Malware Analysis System using Process-Level Virtualization", Proceedings of IEEE Symposium on Computers and Communications, July 2009, pp. 550-556.

[7]. S.T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE Communications Surveys & Tutorials, January 2013, pp. 2046–2069

[8]. O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks," in System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on, pp. 8–pp, IEEE, 2003.

[9]. Gupta Nirbhay,-Improving the Effectiveness of Deceptive Honeynets through an Empirical Learning Approach‖, In the proceeding of Australian Information Warfare and Security Conference, Perth Western Australia 2002.

[10]. Spitzner Lance, "Honeypots: Catching the Insider Threat", In the proceeding of 19th Annual Computer Security Applications Conference (ACSAC), On page(s): 170- 179, December 2003