REVELATION OF INFECTED NODES IN NETWORK USING HONEYPOT

[1]Sabari Giri Murugan S, [2]Shravya R Nadig, [3]Thiyagu S

[1]Assistant Professor, [2]Student of BCA, [3]Assistant Professor
[1]Department of BCA,
[1]Jain Deemed to be University, Bangalore, India.

***Abstract**:* The network which we use for the various purpose may have anonymous nodes that need to be determined detected with a various counter attempt which is done by the unauthorized user (attackers). In this, we use honeypot which can be detected by the intrusion detection system that can be identified the malicious code or activity or software that is performed by the attacker over the network. Further, we can analyze the behavior of different tools that have been created by DOS and DDOS attack over the network. In a DoS defence mechanism, a honeypot acts as a detective server among the pool of servers in a specific network; where any packet received by the honeypot is most likely a packet from an attacker. There are also many loopholes that have been created by the attacker that could be getting information about the legitimate user for his software and hardware requirements.

Index Terms **– Attacker, DoS and DDoS.**

I. INTRODUCTION

In the present fast paced world consistent continuous productive assistance is the establishment for all help associations. The achievement of any new or existing endeavor is basically subject to the unwavering quality and nonstop accessibility of administration. Continuously every individual is getting increasingly more reliant on the web for creative and well-coordinated satisfaction of his need. This increases current standards for greatness unreasonably high for the administration conveyance associations. They should be extra careful subterranean insect while solidifying their security street and rail organize. Various types of dangers and assaults are unendingly attempting to damage their security constitution. One of the most troublesome assaults to forestall is the Distributed Denial of Services (DDoS) Attack since it directly affects the administration accessible to an end-client. Honeypot and Its Types in PC phrasing, a Honeypot is a PC security instrument set to identify, avoid, or, in some way, neutralize endeavors at unapproved utilization of data frameworks. By and large, a Honeypot comprises of information (for instance, in a system site) that has all the earmarks of being an authentic piece of the site, however is really disconnected and checked, and that appears to contain data or an asset of significant worth to assailants, who are then blocked. This is like police sting tasks, casually known as "goading," a suspect. In view of sending, honeypots might be delegated:

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 processing, a forswearing of-administration assault (DoS assault) is a digital assault wherein the culprit looks to make a machine or system asset inaccessible to its planned clients by incidentally or inconclusively upsetting administrations of a host associated with the Internet. Refusal of administration is ordinarily cultivated by flooding the focused on machine or asset with pointless demands trying to over-burden frameworks and avoid a few or every single authentic solicitation from being satisfied. In a dispersed forswearing of-administration assault (DDoS assault), the approaching traffic flooding the unfortunate casualty begins from a wide range of sources. This viably makes it difficult to stop the assault just by obstructing a solitary source. A DoS or DDoS assault is closely resembling a gathering of individuals swarming the passage entryway of a shop, making it difficult for authentic clients to enter, disturbing exchange. Criminal culprits of DoS assaults frequently target locales or administrations facilitated on prominent web servers, for example, banks or Master card installment doors. Vengeance, extortion and activism can propel these assaults.

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.

Even though the last decade has witnessed tremendous growth in the internet service and its use, a proper mechanism has not evolved to discourage or stop the internet attackers. One such internet attack is Distributed Denial of Service (DDoS) attack, which continues to pose a real threat to internet service [1, 2]. Even though many schemes have been proposed to defend against spoofing, DDoS attack [12, 7, 11, 6], none have overcome the difficulties of widespread deployment. Whereas traceback scheme [7, 11, 6, 17] can identify the real source of spoofed attack packets, to take appropriate action against the source: at least to stop them for instances. The pushback mechanism is effective to some extent by enforcing aggregate-based congestion control in the containment of DDoS attack traffic. But it damages the traffic [12] in. Honeypots are physical or virtual machines used to defend information from the warm host [13, 14]. Past years have seen several honeypot mechanisms including a number of roaming schemes. Roaming honeypot schemes are generally used as defence mechanisms against nonspoofed service-level DoS attacks [21]. For a period of time one or more servers may act as honeypot from a pool of servers, without consuming service interruption. In other words, one or more legitimate services in the pool, in coordination with legitimate clients and remaining peer replicas, assumes the role of a honeypot for specific intervals of time called honeypot epoch. Such kind of roaming honeypot services makes difficult for attackers to identify active servers, thereby causing them to be trapped in.

The focus of this paper is to freeze private services from unauthorized sources against address spoofing DDoS attacks. This is achieved by controlling attack traffic to its source using the pushback mechanism, for tracing back to a particular source, and by the ability to defend the attackers using roaming honeypots. The existing system has number flaws namely the honeypot schemes will not work if one of the clients in the AS is an attacker and the other one is a legitimate client; and when there is a physical breakdown in the active path. They have dealt by opening a virtual or physical communication port to any client only after its authentication and for other nodes AS still acts as a virtual/physical honeypot. And by opening a temporary communication channel through the honeypot, by virtually making it act as AS.

Mitigation Strategies

DDoS alleviation is a lot of strategies or apparatuses for opposing or moderating the effect of distributed denial-of-service (DDoS) assaults on systems appended to the Internet by ensuring the objective and hand-off systems. DDoS assaults are a steady risk to organizations and associations by compromising service execution or to close down a site totally, in any event, for a brief timeframe.

The primary activities in DDoS alleviation are to distinguish ordinary conditions for system traffic by characterizing ―traffic patterns‖, which is important for danger identification and alarming. DDoS alleviation likewise requires recognizing approaching traffic to isolate human traffic from human-like bots and commandeered internet browsers. The procedure is finished by looking at marks and analyzing various characteristics of the traffic, including IP tends to treat varieties, HTTP headers, and JavaScript impressions. One system is to pass system traffic routed to a potential objective system through high-limit systems with "traffic scouring" channels.

Manual DDoS alleviation is never again prescribed due to DDoS assailants having the option to go around DDoS relief software that is enacted manually.[3] Best practices for DDoS moderation incorporate having both enemy of DDoS innovation and against DDoS crisis reaction services, for example, Arbor Networks, Incapsula, Allot, Akamai, Cloud Flare or Rad ware. DDoS alleviation is likewise accessible through cloud-based suppliers.

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.

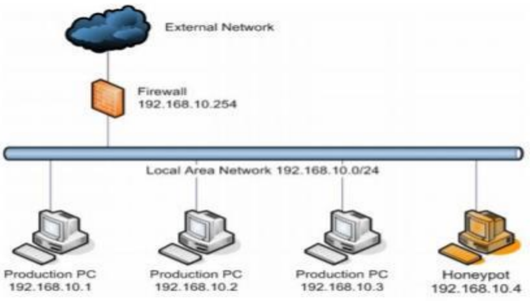


Fig. 1, System Design

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.

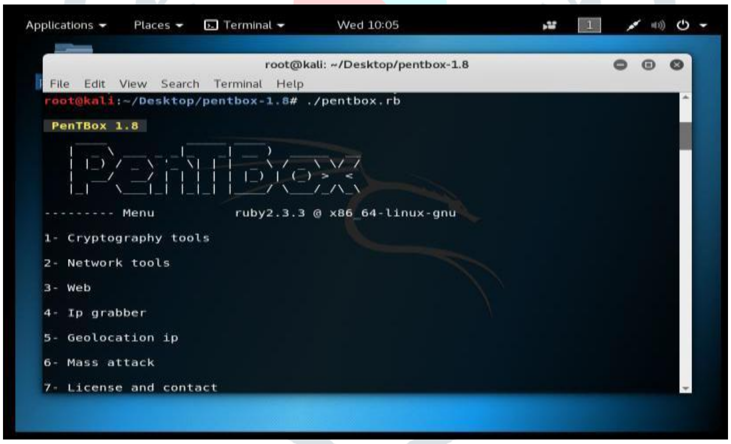
Step 2: Open the command prompt terminal.

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

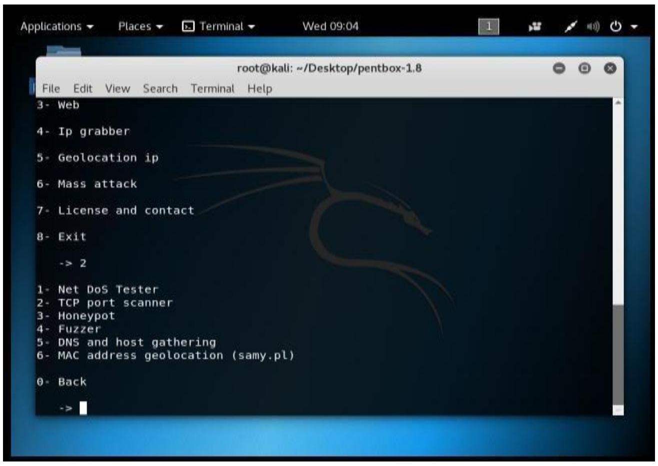

Applications
Places
Terminal
Wed 10:05
root@kali: ~/Desktop/pentbox-1.8
File Edit View Search Terminal Help

```
root@kali:~/Desktop/pentbox-1.8# ./pentbox.rb

 PenTBox 1.8

--------- Menu          ruby2.3.3 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact
```

Fig. 1, Pent Menu

Step 7: Open the Network tools.

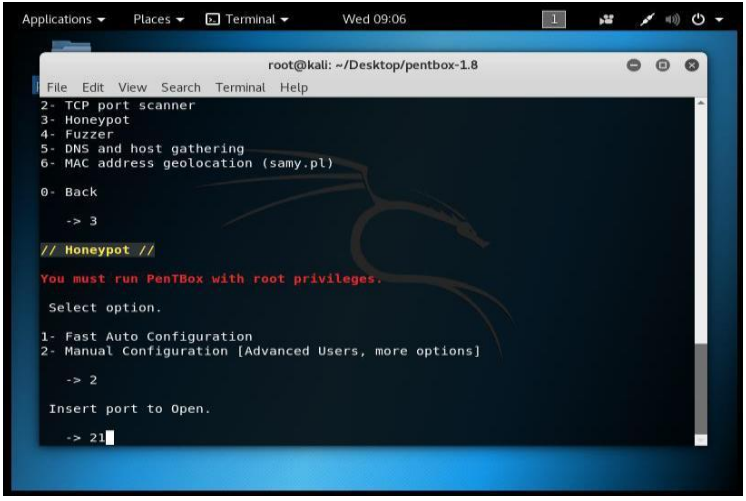
Step 8: Now choose Honeypot option.


Applications
Places
Terminal
Wed 09:04
root@kali: ~/Desktop/pentbox-1.8
File Edit View Search Terminal Help

```
3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   -> 2

1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   ->
```

Fig. 2, Network Tools

Step 9: Now select on which port the honey pot has to be deployed


Applications
Places
Terminal
Wed 09:06
root@kali: ~/Desktop/pentbox-1.8
File Edit View Search Terminal Help

```
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   -> 3

// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   -> 2

 Insert port to Open.

   -> 21
```

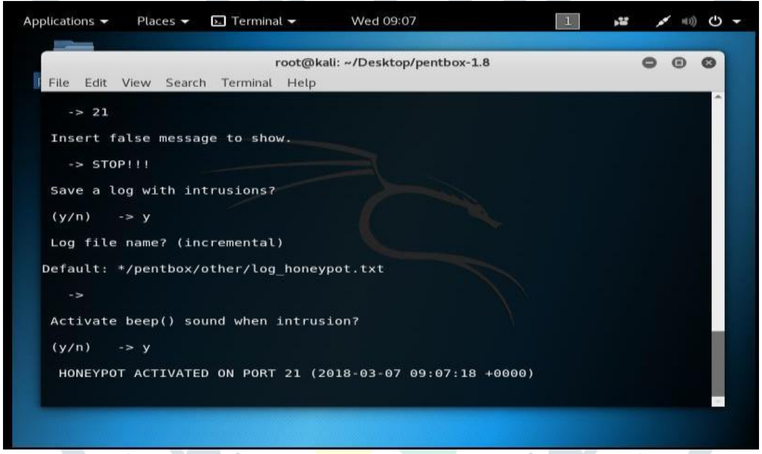
Fig. 3, Honey Pot Deployment

Step 10: 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 11: Now press —y to save the log with intrusions.

Step 12: Now confirm the Log file name. Now press —y to activate beep sound when intrusion is detected.

Step 13: The honey pot is activated on port number 21 that is FTP(Control) port.


Applications
Places
Terminal
Wed 09:07
root@kali: ~/Desktop/pentbox-1.8
File Edit View Search Terminal Help

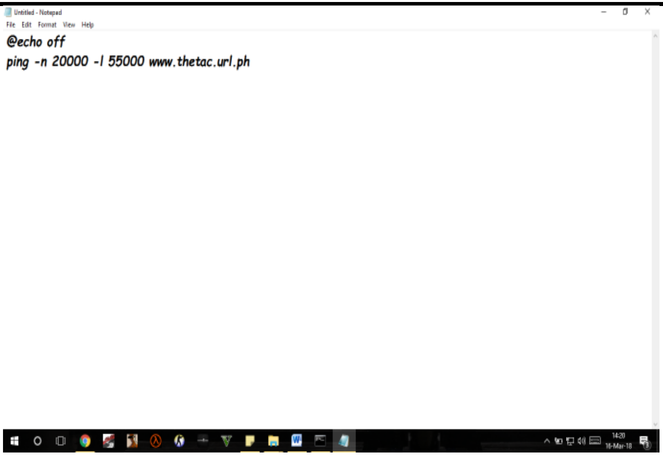
```
   -> 21

 Insert false message to show.

   -> STOP!!!

 Save a log with intrusions?

 (y/n)   -> y

 Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

   ->

 Activate beep() sound when intrusion?

 (y/n)   -> y

  HONEYPOT ACTIVATED ON PORT 21 (2018-03-07 09:07:18 +0000)
```

Fig. 4, Honey Pot Port Activation

Step 14: Now we can able to detect the attack by using honey pot in the activated ports.
Step 15: 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

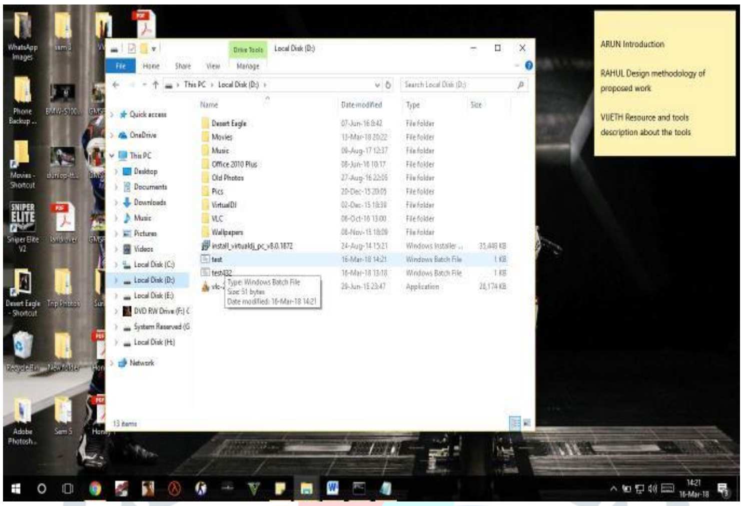
Step 1: Open command Prompt.
Step 2: Ping the website.
Step 3: Create a batch file so that it doesn't display commands.



```
@echo off
ping -n 20000 -l 55000 www.thetac.url.ph
```

Fig. 5, creating a Batch file -Ping Flooding

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



Name	Date modified	Type	Size
Desert Eagle	07-Jun-16 8:42	File folder	
Movies	13-Mar-18 20:22	File folder	
Music	09-Aug-17 12:37	File folder	
Office 2010 Plus	08-Jun-16 10:17	File folder	
Old Photos	27-Aug-16 22:05	File folder	
Pics	20-Dec-15 20:05	File folder	
VirtualDJ	02-Dec-15 18:38	File folder	
VLC	06-Oct-16 13:00	File folder	
Wallpapers	08-Nov-15 18:09	File folder	
install_virtualdj_pc_v8.0.1872	24-Aug-14 15:21	Windows Installer ...	35,448 KB
test	16-Mar-18 14:21	Windows Batch File	1 KB
test432	16-Mar-18 13:18	Windows Batch File	1 KB
vlc-	29-Jun-15 23:47	Application	28,174 KB

Type: Windows Batch File
Size: 51 bytes
Date modified: 16-Mar-18 14:21

ARUN Introduction

RAHUL Design methodology of proposed work

VIJETH Resource and tools description about the tools

Fig. 6, Execute the batch file multiple times

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

CONCLUSION

Dispersed forswearing of administration (DDoS) attacks are hazardous and can possibly render the creation site unusable either by flooding the server associate with a considerable number of poisonous requests or crushing the server by abusing the vulnerabilities in its product. We have successfully recognized the secretive center points in framework by using different strategies like nectar pot to measure the security of the structure and perceive, occupy and check attempts at unapproved use of information systems. Our procedure gives a way to deal with recognize the threatening activities in framework similarly as by using nectar pot we can without a lot of a stretch recognize and strengthen the systems by taking control techniques. Using different gadgets to make a DOS and DDOS ambush in framework, analyzing its lead, and endeavoring to distinguish and direct those sorts of attacks, which can upsets the advantages with the goal that the genuine customers can't get to the administration

FUTURE SCOPE

In this paper, we verified an audit of the DDoS issue, open DDoS ambush gadgets, boundary troubles and norms, and a course of action of available DDoS repugnance instruments. This gives better cognizance of the issue and enables a security official to effectively furnish his store with authentic balancing activity segments for doing combating against DDoS hazard. Programming Defined Networking (SDN) is progressively displacing customary frameworks organization. It is another promising method to manage arranging, constructing and regulating frameworks. In connection with standard coordinated frameworks, SDN enables programmable and dynamic frameworks. Despite the way that it ensures progressively versatile framework the administrators, one should think about present and approaching security threats went with its association. We will probably tear down SDN went with Open Flow show from the perspective of Distributed Denial of Service attacks (DDoS). In this paper, we plot our investigation tends to related to an examination of present and new potential results of affirmation, area and balance of DDoS attacks in this condition.

REFERENCES

[1] Christos Douligeris and Aikaterini Mitrokotsa, "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 Sridhar 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 Honey nets 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