International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

A Hybrid Honeypot Framework for DDOS Attacks Detection and Mitigation

Heidi Melhem[1] *, Yaroub Dayoub[1]
Department of Information Technology,
Faculty of communication and Information Technology Engineering,
University of Tartous, Tartous, Syria.

***Abstract*— Dependency on the internet is escalating day by day, which makes it prone to myriad security threats, for instance phishing, SQL injection, malware and attacks. These threaten one or more of the CIA triad elements, which are Confidentiality, Integrity and Availability. Hence, ensuring continuous security has become an inseparable challenge. These threats could be detected by the classical mechanisms of security such as IDS (Intrusion Detection System), firewalls and antivirus, but after it happens, which means they act as healing tools but do not prevent the threats, also they do not provide detection for new threats, this is where the Honeypot comes in. Honeypot is a trap used to lure possible attackers and interact with them to detour, expose or prohibit per se attacks and to learn new attacker's techniques. This paper presents a hybrid framework consisting of two types of honeypots to relieve the flaws of each type and offer the benefits of both types. Testing this framework with real DDOS (Distributed Denial of Service) attack traffic against a webserver has shown that it is not only practical, but also very efficient by keeping the web server's availability for legitimate users.**

Index Terms*— Hybrid Honeypot, Cybersecurity, DDOS Attack, Detection, Mitigation, victim server, Availability

I. INTRODUCTION

The modern computer field is seeing quick development in online services. These services fill a wide range of needs, to make people's daily life easy and sophisticated. On the other hand, the increasing dependency on these services made it a target for destructive attacks to disrupt the essential technologies, hence leading to service failures. One of the main security threats to internet services and the most risky attack in the world of cyber security is Distributed Denial of Service (DDoS) [1].

The major aim of DDOS attack is to halt the progress of any online administrative application, which is accessed by millions of users, making it impossible to use. The attack targets a variety of network resources, which include websites, servers, and banks [2].

This means DDoS attacks threaten the availability of the CIA triad by flooding the target with an enormous count of requests packets. In order to achieve a high level of security against this kind of attacks, the security tools must not only be concerned with the defense mechanisms but also depend on cunning attackers and take the initiative to notify attacks as soon as they happen. For instance honeypot could be helpful here, which is a trap method that is created and set up to be hacked with the intention of wasting the attacker's resources and time on honeypots rather than attacking real existing systems. [3].

This paper benefits from this concept and uses a development hybrid honeypot to improve network security monitoring, identification, and strengthening system security commonly. The structure of this essay is as follows: in section II, we discuss DDOS attacks. In section III, honeypots are shown. Related works about honeypots under DDOS attack are listed in section IV. After that, we suggested a hybrid honeypots framework in section V. The experimental evaluation is covered in section VI, and the paper's conclusion is provided in section VII.

II. DDOS ATTACK

Most DDOS attacks are conducted from within botnets. A botnet is a collection of numerous PC devices that have been unintentionally brought together, typically due to an infection or other harmful code [4].

The goals of the attack differ according to the attacker's intentions, based on that, we can categorize DDOS attack into the listed below groups: [5]

- Economical or financial gain
- Extortion or retaliation
- Boredom
- Cyber warfare
- Intellectual defy
- Hacktivism
- Ideological doctrine

Due to the different goals of attack, the methods of its occurrence differ, which come into three general classifications: [6]

A. Volumetric attacks (connectionless)

This attack, also known as a 'surge', aims to overwhelm the network's data transmission capacity with a high volume of data that appears to be legitimate, which causes a very slow or nonexistent response. These attacks make up the majority of DDoS attacks and are frequently conducted using a botnet made up primarily of insecure IOT devices.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

B. Protocol attacks

Usually termed as 'TCP state-exhaustion attacks'. Attacks of this kind target processing ability of network infrastructure such as load balancers, firewalls and servers and other components. This happens by exploiting all concurrent connections for layer 3 and layer 4 protocol communications by sending suspicious requests, which will lower the quality of service for legitimate requests.

C. Application attacks (connection based)

These attacks, which are also referred to as 'Layer 7 attacks', aim to establish a connection and exhaust it by consuming exchanges and procedures on the target server or application. Given that only a small number of machines are required to launch an attack, the indicated complex dangers are more difficult to distinguish because of the appearance of real activity at low rates.
The focus of this research will be on the latter type.

III. HONEYPOTS

Effective detection and mitigation of distributed denial of service attacks are crucial because they have the potential to cause harm to a target server. Although complete attack prevention is challenging, a number of techniques have been put forth to mitigate DDoS attacks. The two primary methods for combating DDoS attacks are attack detection and mitigation [7]. Honeypots are useful in both of these methods due to their varieties and capabilities. A honeypot can mimic some or all of a real system's operations and makes it appear to be a part of the network, but it is actually isolated and under close supervision. By relying on this, it records the attacker's activities and allows us to gather valuable information about the attacker's tools and operating procedures [8].

The two broad classifications for honeypots are Low interaction honeypots (LIH) and high interaction honeypots (HIH). High interaction honeypots conduct a variety of tasks and replicate the majority of services found in actual production systems. Although they are difficult to detect and offer greater security, they are significantly expensive to maintain. Low interaction honeypots, on the other hand, mimic the services that attackers frequently use. They are easier to maintain and use fewer resources. On a single physical server, both varieties of honeypots can be implemented as virtual machines [9].
The main functions of honeypots are: [10]

1) Capture new attacks like viruses, worms, etc. To benefit from it in future studies.
2) Luring attackers to attack the system.
3) Protect the production devices by drawing an attacker's attention away from the real network.
4) Gather details about the attacker's equipment, strategies, and tactics.
5) Test the system by determining its risks and vulnerabilities for programs and operating systems that are not yet fully known.
6) Gives highly valuable information by monitoring only the packets that are directed directly at them, so it gathers only a small amount of data.

IV. RELATED WORK

To combat DDOS attacks, several solutions that include honeypots have already been put forth. First, Deshpande et al. [11] use the already-existing infrastructure to cheaply and efficiently build the honeymesh network, which is made up of virtualized honeypots. To separate any attack traffic, a router connects the honeymesh network to the Demilitarized zone (DMZ). The traffic that passes through honeypots is not captured or controlled by this solution. It also needs a safeguard against routers being inundated with malicious requests. Sallowm et al. [12] propose a hybrid honeypot scheme to improve the performance of the traditional IDS, it is achieved by implementing Honeyd systems that mimic real systems and deceive the attackers, also a series of high interaction honeypots and called it honeynets. Honeynets are located behind the Honeyd systems. The scheme does not have any mechanism to analyze the valuable gathered information in the honeynets. And it suffers from a high rate of false positive alerts which wastes the analyst's time. Vishwakarma et al. [13] present a new approach for detecting DDOS attacks in the environment of the Internet of Things (IOT). The approach is based on honeypots and makes use of numerous machine learning techniques. The method uses the data produced by honeypots as an input dataset to train the classifiers of the machine learning model being used. Because machine learning algorithms heavily rely on the training dataset, parameters, and features that are chosen, which require extensive network expertise, they cannot be said to be accurate. They also require routine system updates to keep it operating in a variety of circumstances. The work done by Harikrishnan et al. [14] discusses multiple attack scenarios on a network architecture that contains honeypot and pfsense firewall. The system mitigates attacks by blocking incoming packets based on various firewall rules like geographical IP based blocking, invalid TCP flags, rate limiting, ICMP type based filtering, port blocking and many others. This work depends on the firewall as the first layer of security which is not enough because firewalls are very prone to crash during a DDOS attack.

V. PROPOSED FRAMEWORK

Our work in this paper is similar to the previous references in terms of the honeypot deployments. However, our major contribution in this work is the development of a low interaction honeypot by implementing lightweight scripts written in python programming language using scapy library. Scapy [15] is a powerful library used for packet manipulation, like construct, decrypt, send, capture, match, trace routing, forging and analyzing packets, and sniffing on specific network interface ports. Therefore using scapy helps to enhance the LIH's abilities of detecting DDOS attacks in real time and to guarantee accurate results. In order to maximize their benefits and reduce their drawbacks, we also concentrated on developing a comprehensive framework that combines both low interaction and high interaction honeypots, which also ensures multiple layers of protection. Figure 1 shows the proposed flowchart of our developed hybrid honeypot framework.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

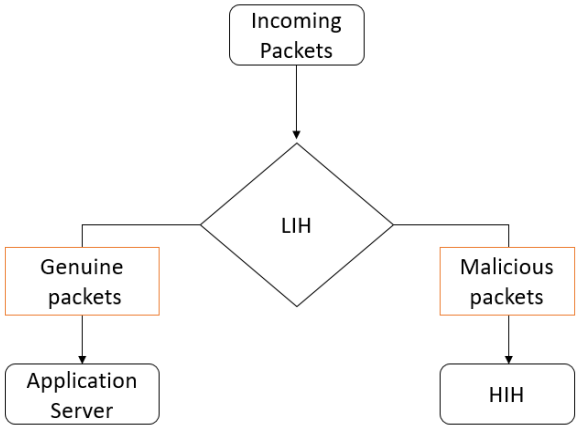

Fig. 1. Flowchart of the proposed method.

The framework relies on low interaction honeypot as the first level of security, it receives all incoming packets to the web server and makes continuous monitoring to check if incoming packets count is high or not compared to a predefined threshold. If no, packets are considered genuine and normally routed to the real web server. Else if yes, LIH considered the system is getting DDOS attack. Hence LIH starts capturing all incoming packets to filter it. The filtering process depends on the IP address. If an IP hits for more than 15 times during 1 sec, then it classifies this packet as a malicious packet and routes it to the second level of security which is the high interaction honeypot to get more information about it and for the analysis process. Else the packet is considered genuine and routed to the real web server to get the service. Thereafter, the LIH gathers the detected malicious packets in a Pcap file as a backup copy about the attack's information, and to analyze it. The routing process for the HIH or the real web server happens using a router, based on an IP list table. The HIH consumes the attacker's resources and time and fails his attempts to harm the service.

VI. EXPERIMENTAL EVALUATION

First we set up the apache server and hosted a simple website and requested it from a good few users. We captured this traffic and analyzed it using wireshark [16], which is a network protocol analyzer that captures network packets and tries to display that packet data as detailed as possible. The obtained traffic is shown in figure 2 which is normal traffic.

Fig. 2. Normal traffic on the web server.

To check the efficiency of the proposed framework, we proceed with two scenarios of DDOS attacks attempts. In the first scenario, we initiated the attack toward the web server with Slowloris tool [17] opens multiple connections to the web server and keeps them open indefinitely while sending intermittent HTTP requests through these connections. The server that is being attacked therefore continues to wait for those fractional attack requests to be finished. The server is protected with traditional security mechanisms like firewall, which identifies the attack based on predefined rules. The first attack scenario was conducted To demonstrate that the attacker had success attacking the web server. The attack's effect was visible in that the web server went down, making it unable to fulfill the real requests from the legitimate client who accessed the website, like in Figure 3 which proves the weakness of the firewall.

```
┌──(kali㉿kali)-[~]
└─$ fping 192.168.1.106
ICMP Host Unreachable from 192.168.1.110 for ICMP Echo sent to 192.168.1.106
ICMP Host Unreachable from 192.168.1.110 for ICMP Echo sent to 192.168.1.106
ICMP Host Unreachable from 192.168.1.110 for ICMP Echo sent to 192.168.1.106
ICMP Host Unreachable from 192.168.1.110 for ICMP Echo sent to 192.168.1.106
192.168.1.106 is unreachable
```

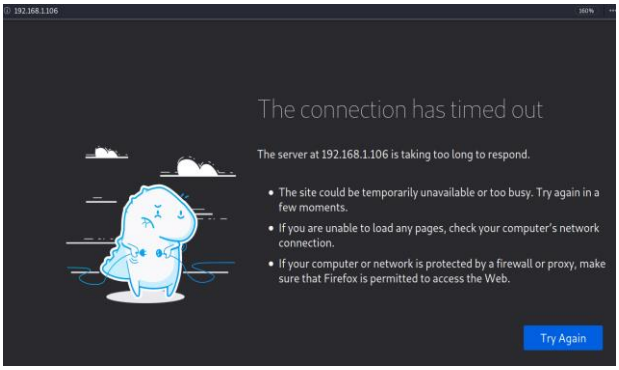

Fig. 3. Web server down.

In the second scenario, we redo the attack after implementing our proposed framework to protect the web server. We made the LIH emulate the web server and open many more ports to deceive the attacker to make him think that the target is easy and not protected, Figure 4 shows the attacker view using nmap scan on the low interaction honeypot.

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp
23/tcp    open  tcpwrapped
80/tcp    open  http         Apache httpd 2.4.49 ((Win64))
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
12345/tcp open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
```

Fig. 4. Nmap scan on LIH.

The python script in LIH sniffs on port 80 to capture DDOS attack traffic, we started the attack using the same tool, and made other users request the web site during the attack process. We noticed that the security system is working properly because the majority of legal users get the requested web page. And the web server continues to work although it is getting a DDOS attack which frustrates the attack attempts. The filtration process is successful with a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

low margin of error. Figure 5 shows the traffic on the fortified web server during the second scenario.

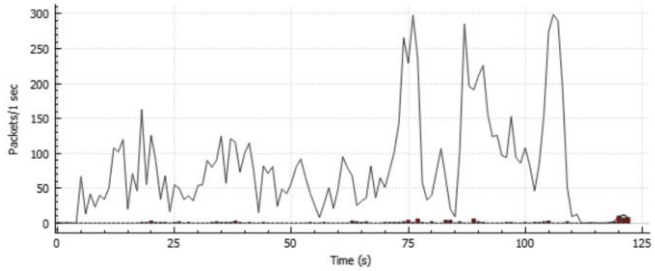

Fig. 5. Traffic on fortified web server.

The final stage of our work includes analyzing the packets of DDOS traffic using wireshark in the high interaction honeypot. The analysis gives us this data for every packet: serial number, time, length, source and destination IP address, source and destination port number. Which is shown in figure 6. That helps us observe the packets closely and block specific IP addresses.

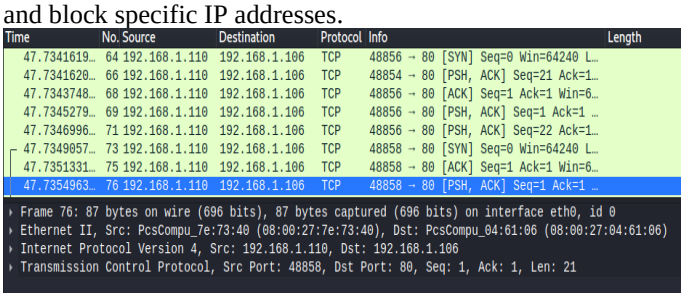

Fig. 6. Analyzing DDOS attack in HIH.

The most important advantage of the proposed framework is that true positive rate (TPR) and the false positive rate (FPR) reached logical proportions, and they can be calculated using the following equations: [12]

$$TPR = TP / (TP + FN). \quad (1)$$

And

$$FPR = FP / (FP + TN). \quad (2)$$

Where:

FP: False Positive

FN: False Negative

TN: True Negative

TP: True Positive

and Table 1 provides definitions for these terms:

TABLE I
ALERTS DURING ATTACKS TERMS

Attacks	Alerts	
	Yes	**NO**
YES	TP	FN
NO	FP	TN

VII. CONCLUSION

The proposed framework has many advantages manifested in detecting DDOS attacks and mitigating the negative impact of it. The detection happens in real time by implementing python script in the low interaction honeypot which enhances its capabilities. As well as the use of hybrid honeypot architecture provided many levels of security which mitigates the harmful impact of the attack. Besides that, the tested results are highly accurate and the whole proposed framework helps enhance the rate of true positives and reduce the rate of false positives, compared to previous studies. This framework is not resource consuming, does not require extensive network expertise, and easy to implement in any desired environment.

Data Availability The dataset generated and analyzed for the current study is not publicly available due to privacy reasons but is available from the author on reasonable request.

DECLARATIONS

Ethical statement Not applicable.

Consent statement Not applicable.

Conflict of interest statement On behalf of all authors, the corresponding author states that there is no conflict of interest.

Funding The authors did not receive support from any organization for the submitted work.

AUTHOR CONTRIBUTIONS

All authors contributed to the study conception and design. Heidi Melhem and Prof. Yaroub Dayoub performed material preparation, data collection and analysis. The first draft of the manuscript was written by Heidi Melhem and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

REFERENCES

[1] K. M. Prasad, A. R. Reddy, And M. G. Karthik, "Flooding Attacks To Internet Threat Monitors (Itm): Modeling And Counter Measures Using Botnet And Honeypots," *Ijcsit. International Journal Of Computer Science & Information Technology*, Vol. 3, No. 6, Pp. 159–172, Dec. 2012, Doi: 10.5121/ Ijcsit.2011.3612.

[2] M. Mirza, M. Usman, R. P. Biuk-Aghai, And S. Fong, "A Modular Approach For Implementation Of Honeypots In Cyber Security," *Ijaer. International Journal Of Applied Engineering Research*, Vol. 11, No. 8, Pp. 5446–5451, Nov. 2016.

[3] Q. Nasir And Z. Al-Mousa, "Honeypots Aiding Network Forensics: Challenges And Notions," *Jcm. Journal Of Communications*, Vol. 8, No. 11, Pp. 700–707, Nov. 2013, Doi: 10.12720/Jcm.8.11.700-707.

[4] Y. Lu And M. Wang, "An Easy Defense Mechanism Against Botnet-Based Ddos Flooding Attack Originated In Sdn Environment Using Sflow," In *Proc. Acm Int. Conf. Future Internet Technologies (Cfi)*, Nanjing, China, June 2016, Pp. 14–20.

[5] S. T. Zagar, J. Joshi, And D. Tipper, "A Survey Of Defense Mechanisms Against Distributed Denial Of Service (Ddos)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

Flooding Attacks," *Ieee Commun. Mag.*, Vol. 15, No. 4, Pp. 2046–2069, Mar. 2013.

[6] R. Selvaraj, V. M. Kuthadi, And T. Marwala, "Ant-Based Distributed Denial Of Service Detection Technique Using Roaming Virtual Honeypots," *Iet Communications*, Vol. 10, No. 8, Pp. 929–935, May. 2016.

[7] Y. S. Shegaonkar, L. Patil, And S. Zade, "Survey On Multilevel Security Using Honeypot," *Ijisrt. International Journal Of Innovative Science And Research Technology*, Vol. 6, No. 5, Pp. 959–963, May. 2021.

[8] R. C. Joshi And A. Sardana, "Honeypots," In *Honeypots: A New Paradigm To Information Security*. Boca Raton, Fl, Usa: Crc Press, 2011, Pp. 7–9.

[9] L. Spitzner, "Classifying Honeypots By Level Of Interaction," In *Honeypots: Tracking Hackers*. Boston, Massachusetts, Usa: Addison-Wesly, 2003, Pp. 87–96.

[10] N. Naik, P. Jenkins, N. Savage, And L, Yang, "A Computational Intelligence Enabled Honeypot For Chasing Ghosts In The Wires," *Complex & Intelligent Systems*, Vol. 7 , No. 1, Pp. 477–494, Nov, 2020.

[11] H. A. Deshpande, "Honeymesh: Preventing Distributed Denial Of Service Attacks Using Virtualized Honeypots," *Ijert. International Journal Of Engineering Reseach & Technology*, Vol. 4, No. 8, Pp. 263–267, Aug. 2015, Doi: 10.17577/ Ijertv4is080325.

[12] H. Sallowm, M. Assora, M. Alchaita, And M. Aljindi, "A Hybrid Honeypot Scheme For Distributed Denial Of Service Attack," *Ajece. American Journal Of Electrical And Computer Engineering*, Vol. 1, No. 1, Pp. 33–39, May. 2017, Doi: 10.11648/J.Ajece.20170101.15.

[13] R. Vishwakarma And A. K. Jain, "A Honeypot With Machine Learning Based Detection Framework For Defending Iot Based Botnet Ddos Attacks," In *Proc. Ieee Int. Conf. Trends In Electronics And Informatics (Icoei)*, Tirunelveli, India, Apr 2019, Pp. 1019-1024.

[14] V. Harikrishnan, H. S. Sanket, K. S. Sahazeer, S. Vinay, P. B. Honnavalli, "Mitigation Of Ddos Attacks Using Honeypot And Firewall," In *Proc. Springer Int. Conf. Data Analytics And Management (Icdam)*, Jelenia Gora, Poland, June 2022, Pp. 625-635.

[15] S. Bansal And N. Bansal, "Scapy–A Python Tool For Security Testing," *Journal Of Computer Science & Systems Biology*, Vol. 8, No. 3, Pp. 140159, Mar .2015, Doi: 10.4172/Jcsb.1000182.

[16] H. Iqbal And S. Naaz, "Wireshark As A Tool For Detection Of Various Lan Attacks," *Jcse. International Journal Of Computer Science And Engineering*, Vol. 7, No. 5, Pp.833-837, May. 2019.

[17] T. Shorey, D. Subbaiah, A. Goyal, A. Sakxena, And A. K. Mishra, "Performance Comparison And Analysis Of Slowloris, Goldeneye And Xerxes Ddos Attack Tools," In *Proc. Ieee Int. Conf. Advances In Computing, Communications And Informatics (Icacci)*, Bengaluru, India, Sep 2018, Pp. 318-322.