A Distributed Cloud Honeypot Architecture

Jason Xiaojun Huang
School of Computing
University of Portsmouth
Portsmouth, England
Xiaojun.Huang@port.ac.uk

Shikun Zhou
School of Computing
University of Portsmouth
Portsmouth, England
Shikun.Zhou@port.ac.uk

Nick Savage
School of Computing
University of Portsmouth
Portsmouth, England
Nick.Savage@port.ac.uk

Weicong Zhang
School of Computing
Zhejiang Wanli University
Zhejiang, China
zhangweicong@zwu.edu.cn

***Abstract*— Distributed denial of service (DDoS) attacks pose a huge threat to the Internet. Follow the rapid usage of the Internet of things (IoT), the DDoS attack is no longer a mere traffic attack, the original attack on the application layer surpasses the attack on the network layer. Furthermore, DDoS attacks using Bonnets result more destructive effects. This research aims to propose a new collaborated active defense framework between Honeypot and cloud platform to detect and defend future DDoS attacks in the context of the IoT with the instantaneous malicious traffic measured in Terabytes.**

Keywords—DDoS attacks, Bonnets, Honeypot, Cloud computing

I. INTRODUCTION

Distributed denial of service (DDoS) attacks pose a huge threat to the Internet. Defence mechanisms emerge and develop rapidly. However, attackers constantly develop and improve their malicious methods, technologies and tools to attack and fool these security systems. The DDoS attacks become more and more complicated and destructive, reaching its turning point where revolutionary technologies and corroborated efforts are needed.

This research will explore and propose a new active defence architecture based on the cloud architecture and decoy servers, Honeypots to detect, defend and analyse evolving DDoS combined attacks.

II. BACKGROUND

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 [1]. 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 distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers [2].Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic. A botnet is a network of zombie computers programmed to receive commands without the owners' knowledge [3].

Common DDoS attacks stream an abnormal volume of packets to the victim, targeting critical network resources, thus making it unavailable to legitimate users. More complicated DDoS attacks send incorrectly formatted packets, cluttering applications or protocols on the victim machine and forcing them to freeze or restart [4]. Modern DDoS attacks are more sophisticated and powerful than other cyber-attacks.

Honeypot is the network security supplement active defence system. It can capture attacks, record intrusions about tools and hacking activities, and prevent attacks from flowing out of compromised systems. As the single most effective active defence against DDoS attacks, it can defend large operational network with a high probability against known DDoS and against new, future variants. Moreover, it can be used to trap the attacker so that recording of the compromise can help in a legal action against the attacker [5].

However, the latest development of the DDoS attacks results in extreme scales and severities beyond the capacity of a single Honeypot. Especially, those DDoS attacks using a large number of bonnets can easily reach a few Tbps traffic. Some examples will be given later. This is equivalent to a cloud-based DDoS attack using many distributed hosts, i.e. bonnets. Therefore, if a single Honeypot can't cope with the cloud-based DDoS attack, Cloud-based Honeypots are proposed to tackle with cloud-based DDoS attacks.

III. DDOS ATTACKS

A distributed denial of service (DDoS) attack launches a coordinated DoS attack against one or more targets using multiple hosts under client/server mode. Usually criminals use multiple hijacked host computers, Botnets, as an attack platform, thereby greatly increasing the impact of the attack [6]. Distributed denial of service (DDoS) attacks aim to flood victims with unusual traffic, preventing or blocking legitimate network users to access network resources. DDoS attacks occupy considerable bandwidth to attack a large opponent, such as a web based, media company. Such attacks often command thousands of hijacked hosts, Botnets to send traffic

to the victim simultaneously [7], making the victim's network unusable, or greatly deteriorated network performance.

Common DDoS attacks stream an abnormal volume of packets to the victim, targeting critical network resources, thus making it unavailable to legitimate users. More complicated DDoS attacks send incorrectly formatted packets, cluttering applications or protocols on the victim machine and forcing them to freeze or restart [4]. Modern DDoS attacks are more sophisticated and powerful than other cyber-attacks. Common DDoS attacks can be classified into three major categories [8]:

- Volume based attacks: these include ICMP floods, UDP floods and other spoofing packet attacks. The primary target is to block the victim's site bandwidth. This type of attacks could easily exceed the maximum capacities of most single means of defence, including Honeypots. Hence, this category will be the main focus on this work.
- Protocol based attacks: this type covers mainly SYN flooding, fragmented packed attacks, Ping of death, and Smurf attack. This type of attack's primary target the actual server resources, such as firewall.
- Application layer attacks: this type of attacks target on web applications and are considered to be most sophisticated and destructive type.

Some specific DDoS attacks belonging to each category are presented in Figure 1. DNS Amplification attacks are a typical example of the Volumetric attack. Attacks target to DNS server. An attack starts with a spoofed IP address and lures a victim DNS server with responding to a large amount of data, which degrades the service of DNS server [9]. This type of DDoS attacks will commonly exceed the maximum capacity of most of defence means, including single Honeypots. For example, GitHub suffered the worst DDoS attack ever, reaching a top attacking traffic at 1.35 Tbps. It is also the largest and most powerful distributed denial of service (DDoS) attack in the history of the Internet [10].

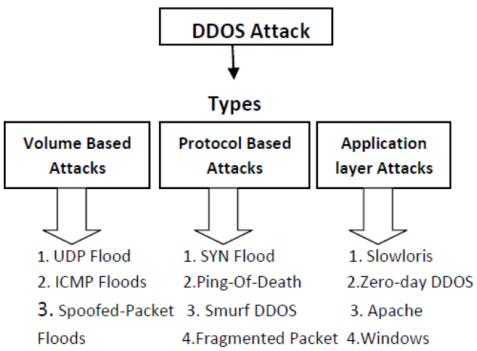

Fig. 1. The Classificaiton to DDoS Attacks

As a result, there will not be any single means of defence, including Honeypot, can tackle or even simply copy with such volume of traffic. Cloud computing platforms provide a possible means to collaborate several single means of defence, especially a collection of collaborated Honeypots, to defend DDoS attacks with high traffic volumes. Moreover, because cloud computing is merely dependent on computer networks, it is very vulnerable to DDoS attacks. In [5] research, the author uses Honeypot to rebuild his cloud computing architecture, and fully demonstrates that Honeypot can resist known DDoS attacks and new, future variants, as well as providing more effective legal proof function.

IV. DDoS AND HONEYPOTS

Active defence is a strategy of implementing different security measures to attack potential intruders. This strategy is based on the assumption that the potential intruder under attack is less capable. Examples of this policy include creating and using lists of trusted networks, devices, and applications, blocking untrusted addresses, and vendor management.

Honeypot is the network security supplement active defence system. It can capture attacks, record intrusions about tools and hacking activities, and prevent attacks from flowing out of compromised systems. As the single most effective active defence against DDoS attacks, it can defend our operational network with a high probability against known DDoS and against new, future variants. Moreover, it can be used to trap the attacker so that recording of the compromise can help in a legal action against the attacker [5].

In computer security, a Honeypot is a program or a server voluntarily made vulnerable in order to attract and lure hackers. The attackers who think they are targeting a real resource behave "normally", using their attack techniques and tools against this lure site, which allow the defenders to observe and monitor their activities, analyse their attacking methods, learn and prepare the adequate defences for the real resources [11].

The Honeypot is simply a system for trapping attacks. The concept of Honeypot firstly appeared in Clifford Stoll's novel "The Cukoo's egg". In addition, the Honeypot is described as "A security resource who's value lies in being probed, attacked or compromised" [12]. Overall, a Honeypot is a fake disguised system with carefully engineered vulnerabilities. It can be a network, a host or a service. In the field of computer security over the past few years, Honeypot have proven to be a good source of research into a wide variety of malware and its variants. The first practical Honeypot tool appeared in the late 1990s as a "The Deception Toolkit", developed by Fred Cohen in 1998, They have since become available for both public and commercial use, particularly for dealing with self-replicating programs, or worms [13].

According to the different interaction frequency between Honeypot and attacker, it can be divided into *high interaction Honeypot* and *low interaction Honeypot*. Moreover, Honeypots can be divided into *production Honeypot* and *research Honeypot* depending on the ultimate purpose of the deployment. Otherwise, there is a classification method that can divide Honeypot into *physical Honeypot* and *virtual Honeypot* based on different design schemes [14]. A comparison is included in Fig. 2.

High-Interaction	Low-Interaction
Real services, OS's, or applications	Emulation of TCP/IP stack, vulnerabilities, and so on
Higher risk	Lower risk
Hard to deploy and maintain	Easy to deploy and maintain
Capture extensive amount of information	Capture quantitative information about attacks

Fig. 2. Advantages and Disadvantages of High- and Low- Interaction Honeypots

Compared with intrusion detection system (IDS) and other technologies, Honeypot technology is relatively simple, making it easier for network managers to grasp some information of attackers. A comparison between Firewalls and Honeypots is given in Fig. 3. Another comparison between IDS and Honeypots is given in Fig. 4.

The main features or components of Honeypots are *network spoofing function*, *port redirection*, *alerting*, *data capture, analysis, and control.*

Network Spoofing - The Honeypot is a decoy system designed to be attacked. It is ostensibly made into a real host that lures attackers. It simulates operating systems or various vulnerabilities on the spoofed host, generates simulated network traffic, and induces intruders to attack.

Port Redirection - Honeypots deploy port redirection technology to simulate services in a working system without actually offering services to real users. The component, Port Redirector module mainly transmit traffic from a production server to a deception server.

Alerting – a Honeypot has an essential alerting module, notifying administrators and other security professionals in real-time.

Firewall	Honeypot
It is design to keep intruders out of the network.	It is design to lure intruders to attack on the system.
Only authorized traffic will be allowed to pass.	It allows all traffic to interact with the honeypot system.
Placed at network's traffic entering points.	Placed inside the network as mimic the original production servers
Logs of incoming and outgoing traffic are maintained, so contains more entries.	Maintain the logs of interacted traffic only, so collect fewer entries.
It cannot protect from internal threats and from attacks that bypass the firewall.	It can protect from internal threats, information gathering is our prime aim.
According to purpose various firewalls are used i.e. packet filter, application level gate-ways and circuit level gateways.	According to purpose two types of honeypots are used i.e. production honeypot, research honeypot.

Fig. 3. A Comparison between Firewalls and Honeypots

IDS	Honeypot
A system silently monitors the network's traffic and gives alerts to tell about the kind of intruders based upon the database of existing intruders.	It is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information system.
IDS require signatures for detecting malicious activities.	Honeypot does not require any signature for detection.
IDS is fail to detect attacks if they are unknown at the time of its deployment.	Honeypots can detect vulnerabilities that are not yet understood or known.
Easy to deploy as it does not affect existing infrastructure.	Deployment complexity is based on type and purpose for which it developed.
It is suffer from the problem of false alerts like false positive and false negative.	It collects information about strategy used and generates alert when intruder try to compromise it, so overcome false alert problem.
According to monitoring scope in terms of area covered, it has two main types Network based IDS, Host based IDS	According to interaction with intruders it can be divided as low, medium and high interaction honeypots.

Fig. 4. A Comparison between IDS and Honeypots

Data Control – Honeypots control all network activity to prevent intruders from using the spoofing system as a springboard to attack other systems. They also control the system's data traffic without being suspected by the intruder. After an intruder occupies a system, it may make a network connection, and download some toolkits to launch attacks on specific targets, so the intruder must be given some "legitimate" permissions.

Data Capture and analysis - all activities that enter and exit the Honeypot are monitored and recorded with as much information as possible being captured to analyse the attacker's strategy and motivation. The captured data cannot be placed on the host of the Honeypot, otherwise it will be easily found by intruders.

Dwiyatno and his fellow researchers [15]used Honeyd Honeypot to detect DDoS attacks in the research. The experimental results prove that the data collected by Honeyd Honeypot can detect DDoS attacks in real time. [16] used virtual Honeypots to detect DDoS attacks effectively. [17] applied Honeypot-based redirection technology which effectively prevent the occurrence of DDoS attacks and maintain QoS at the ISP level whilst maintaining usual response times of legitimate users during DDoS attacks.

Through a rigorous review of previous research, we can find that DDoS attacks have begun to undergo serious changes. Among them, the botnet group consisting of IoT devices has begun to grow larger and larger. Mirai IoT botnets have become synonymous with new botnets [18]. Furthermore, the use of public resources to implement the amplified reflection attacks of DDoS attacks has become more and more common. Attackers nowadays creates immensely huge spam traffic to attack networks and their services, using collaborate attacks and hybrid attacks. A single Honeypot cannot cope with even growing huge volumes of attack traffic. In addition, the emergence of combined and collaborated DDoS attacks stop an ordinary Honeypot to detect them quickly and efficiently. Therefore, it is necessary to design a collaborated Honeypot architecture which can effectively

tackle vast volume of DDoS traffic whilst carrying a large amount of detecting, data capturing and analysis tasks simultaneously. In result, A cloud-based collaborated Honeypot infrastructure is proposed in this work.

V. CLOUD HONEYPORT INFRASTRUCTURE

There is a new concept of Cloud Security which had been introduced by CISCO in Cloud services [19]. It manages security for the Cloud and protects users and protects data and applications in the cloud [19]. The major Cloud Security functions include:

- Detect and prevent threats
- Protect Cloud and its users
- Secure Cloud data and application

Among the CISCO Cloud Security, Cisco Cloudlock is a cloud-native cloud access security broker (CASB) and cloud cybersecurity platform. It protects users, data, and apps across software as a service, platform as a service, and infrastructure as a service [20]. However, the current CISCO Cloud Security does not include Honeypot services. Moreover, CISCO Cloud Security construction cost is rather high, therefore generally small to medium-sized enterprises cannot afford such infrastructure by their own. Hence, this work starts from proposing a Honeypot scheme based on cloud architecture, namely, *Cloud Honeypot*, to achieve its unique security functionalities, and to offer it as an active defense security service to small and medium-sized enterprises. Cloud Honeypot will further be able to tackle DDoS attacks with extreme traffic loads, such as the incident mentioned earlier on reaching a 1.35 Tbps bandwidth [10]. This design can deploy a "Cloud of Honeypots" to defend against DDoS attacks using a "Cloud of Botnets". This research will also create a new business model for widely expanding the usage of the Cloud Computing concepts, which will be reported in another paper in writing. The design of the Cloud Honeypot and the developed business model are currently in the process of applying for relevant patents. Therefore, some of confidential details will not be discussed in this paper. A general Cloud Honeypot architecture is presented in Fig. 5.

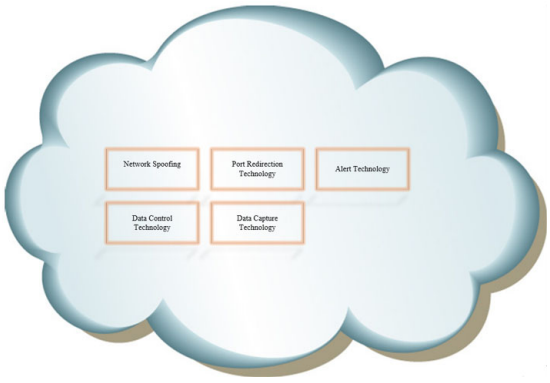

Fig. 5. An Initial Cloud Honeypot Architecture

In addition, due to the emergence of hybrid attacks, such as Dyn's DNS server attack [21], two different attack methods have been found. The hybrid type of attacks are difficult to be fully captured and analysed by a single Honeypot, due to its complexity. In response to this problem, Cloud Honeypot splits the ordinary Honeypot framework into four collaborated modules, which are implemented and coordinated using virtualised solutions. Each analysis module will generate its own system log and the Cloud Honeypot will later combine and analyse them later. In addition, it is need to include a new module, DDoS feature detection module, for DDoS feature matching to prevent false positives and help the analysis of future DDoS attacks. A modified Cloud Honeypot is presented in Fig. 6.

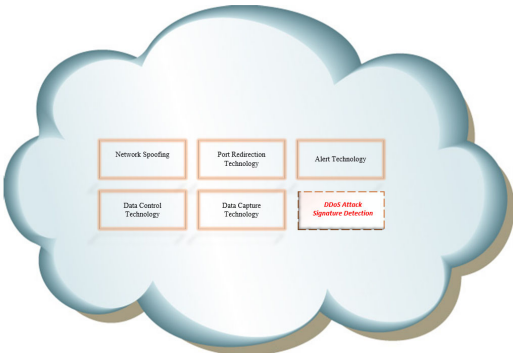

Fig. 6. A Modified Cloud Honeypot Architecture

In order to ensure the security of the new cloud Honeypot itself and further improve the capacity, reliability, and scalability of the system, this architecture deploys multiple Cloud sub-Honeypots to the whole production system. The improved system will further confuse the DDoS attacker's perception of the Honeypot itself, as well as effectively combining with IDS to improve detection performance. In addition, suspicious traffic detected from the IDS will be randomly allocated to any available Cloud sub-Honeypot for containing, data capturing and analysing. After retaining and analysing attack traffic, the final system logs will be transfer to cloud storage for future research and analysis. The design of the main processes of Cloud Honeypot is presented in Fig. 7.

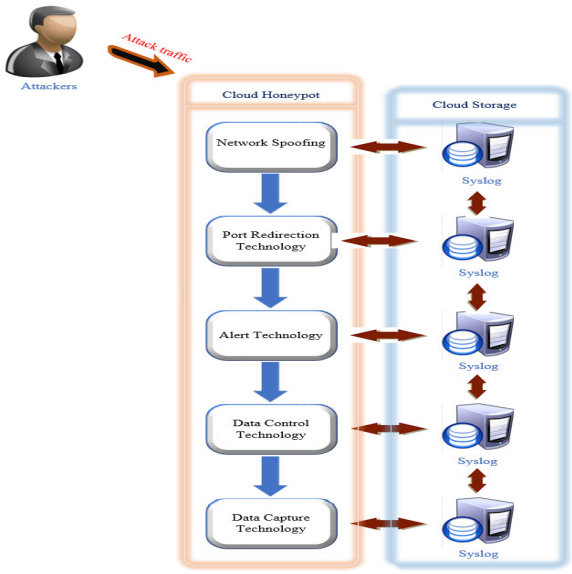

Fig. 7. Cloud Honeypot Diagram

VI. INITIAL IMPLEMENTAION AND PROTOTYPING

The first stage of the work is to use a simulator, namely, EVE-NG [22], to simply build a network architecture based on Honeypot detection. In addition, a penetration study software, Kali Linux system [23], is used to simulate DDoS attack to test Honeypot server and analyse the result of Honeypot server's detection response. In order to simulate the experimental environment more realistically, EVE-NG simulator was used to build the network architecture and VMware platform, vSphere [24] was used to build the Honeypot server, and Kali Linux system was used to simulate the DDoS attack. The first stage of the experiments has been completed and the experimental Cloud Honeypot is shown in Fig. 8. A simulated attack on a full network server using Kali Linux is presented in Fig. 9.

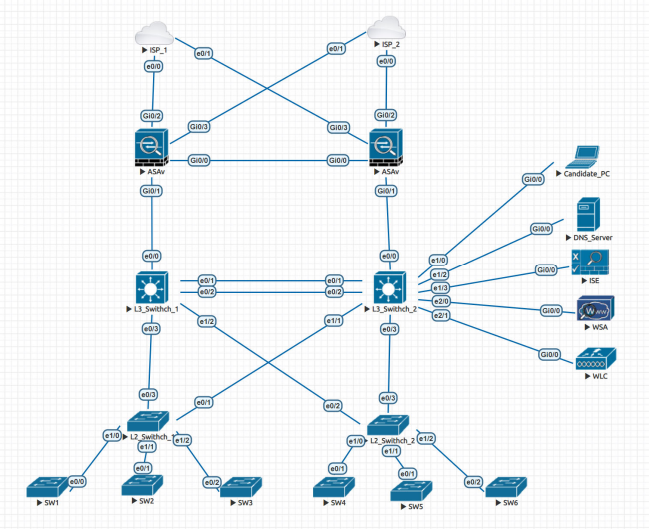

Fig. 8. Stage 1 Experimental Cloud Honeypot

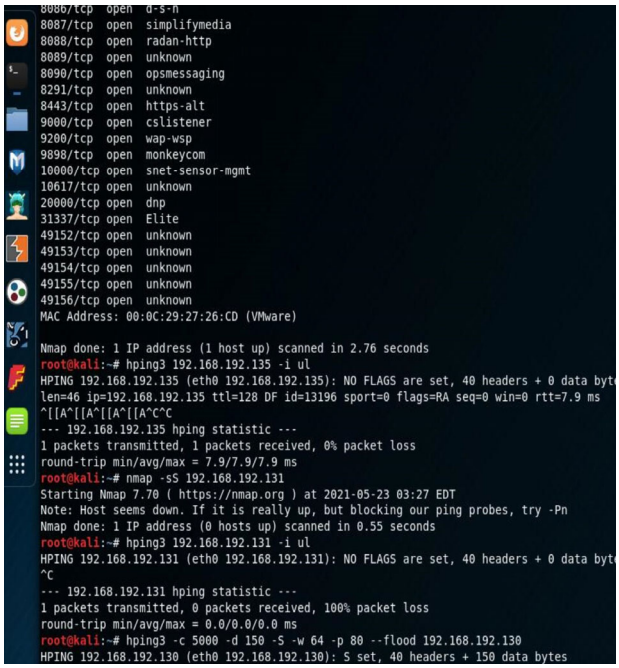

Fig. 9. A simulated attack on a full network server

Fig. 10 shows the Cloud Honeypot detecting the Kali Linux Server and its malicious behaviours on the same LAN and alerting the corresponding events.

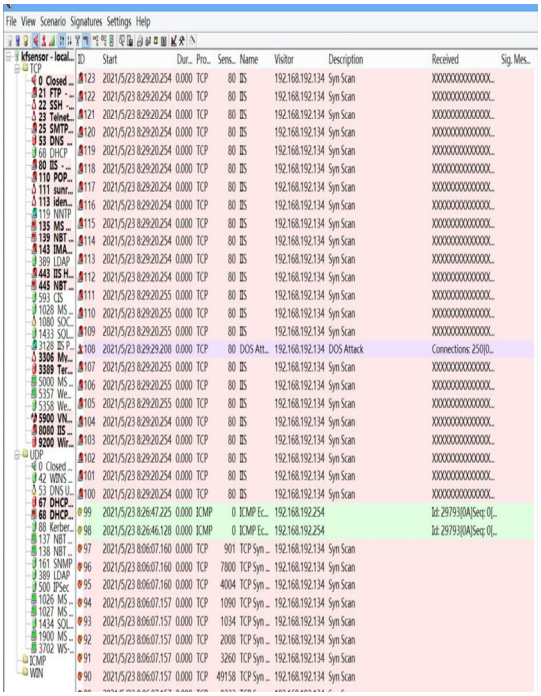

Fig. 10. Penetration Study Outputs

The second stage will use virtual technology to build multiple platforms to simulate each function of Honeypot and integrate multiple platforms to build a cloud Honeypot. Stress test it with Kali Linux.

Further stages will run a complete, small scale Cloud Honeypot in a real environment. Several other DDoS attack

tools will be identified and used to test the Cloud Honeypot. This test will observe the ability of Cloud Honeypots to catch attacks and detect the performance of attacks, as well as further improve the design of the framework.

VII. CONCLUSION AND WHAT'S NEXT

This work proposes and develops a new cloud security concept using Cloud infrastructure. It started with a comprehensive investigation to the current status of DDoS attacks, especially the category of volume based DDoS attacks. A thorough review has been done to the most effective detection and active defense scheme, Honeypot. The major identified problem of existing Honeypots is lack of enough computational power to tackle serve volume based DDoS attacks, especially those using Botnets, i.e. a Cloud style DDoS attack. It is found that although a single Honeypot can't cope with DDoS attacks exceeding its maximum capacity, but an enough number of collaborated Honeypots can deal with this type of DDoS attacks. Further considering the rapid development of Cloud security infrastructure, the work proposed a new Cloud Honeypot infrastructure, as well as a newly developed business model for cloud computing. The first stage of such design and implementation based on major industry simulation packages has been completed and relevant sample results have been reported in this paper. The next stages of the work will involve further development of Cloud Honeypot collaborating modules, data analysing functions and more cooperative sub-Honeypots in the structure. A new concept of Honeypots as a Service (HaaS) has been proposed and developed as well, which will be reported in another paper in progress. The HaaS concepts will be used to further develop the Cloud Honeypot infrastructure.

REFERENCES

[1] CISCO, "Defending aganist today's critical threats," 2019.

[2] D. Zargar, S. T., Joshi, J., & Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," IEEE Commun. Surv. Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013.

[3] Cloudbric, "Has Your Website Been Bitten By a Zombie?," 2019. https://www.cloudbric.com/blog/2015/08/has-your-website-been-bitten-by-a-zombie/.

[4] P. Mirkovic, J., Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," Comput. Commun. Rev., 2004.

[5] K. Shridhar and N. Gautam, "A Prevention of DDos Attacks in Cloud Using Honeypot," Int. J. Sci. Res., pp. 2319–7064, 2014, [Online]. Available: https://www.ijsr.net/archive/v3i11/T0NUMTQxNTQ0.pdf.

[6] N. Weiler, "Honeypots for distributed denial-of-service attacks," in Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE, 2002.

[7] J. Nazario, "DDoS attack evolution," Netw. Secur., 2008.

[8] M. Malik and Y. Singh, "A Review: DoS and DDoS Attacks," Int. J. Comput. Sci. Mob. Comput., vol. 4, no. 6, pp. 260–265, 2015.

[9] CLOUDFLARE, "What is a DDoS Attack?" https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

[10] L. Newman, "A 1.3-Tbs DDoS Hit GitHub, the Largest Yet Recorded," wired.com, 2018. https://www.wired.com/story/github-ddos-memcached/.

[11] C. K. Ng, L. Pan, and Y. Xiang, "Introduction to Honeypot," in Honeypot Frameworks and Their Applications: A New Framework, Springer, Singapore, 2018, pp. 1–5.

[12] L. Spitzner, "The Value of Honeypots, Part One: Definitions and Values of Honeypots," Honeypots: concepts, approaches, and challenges, 2001.

[13] R. Vishwakarma and A. K. Jain, "A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks," in Proceedings of the IEEE International Conference on Trends in Electronics and Informatics, ICOEI 2019, 2019, pp. 1019–1024.

[14] G. Vasile and O. Cangea, "Study of Honeypot Technology for Virtual Space Monitoring-Conpot Operation," Pet. Univ. Ploiesti Bull. Tech. Ser., vol. 70, no. 1, 2018.

[15] S. Dwiyatno, A. P. Sari, A. Irawan, and S. Safig, "PENDETEKSI SERANGAN DDoS (DISTRIBUTED DENIAL OF SERVICE) MENGGUNAKAN HONEYPOT DI PT. TORINI JAYA ABADI," J. Sist. Inf. dan Inform., vol. 2, no. 2, pp. 64–80, 2019.

[16] R. Venkatesan, G. Ashwin Kumar, and M. Ragu Nandhan, "A NOVEL APPROACH to DETECT DDOS ATTACK THROUGH VIRTUAL HONEYPOT," in IEEE International Conference on System, Computation, Automation and Networking, ICSCA 2018, 2018.

[17] N. S. Rao, K. C. Sekharaiah, and A. A. Rao, "A survey of distributed denial-of-service (DDoS) defense techniques in ISP domains," in Innovations in Computer Science and Engineering, Springer, Singapore, 2019, pp. 221–230.

[18] CLOUDFLARE, "What is the Mirai Botnet?," 2021. https://www.cloudflare.com/en-gb/learning/ddos/glossary/mirai-botnet/.

[19] CISCO, "Cloud Security Products and Solutions," 2020. https://www.cisco.com/c/en_uk/products/security/cloud-security/index.html.

[20] CISCO, "CISCO Cloudlock," 2021. https://www.cisco.com/c/en_uk/products/security/cloudlock/index.html.

[21] Dyn, "Dyn Status Updates Oct 2016," 2016. https://www.dynstatus.com/incidents/nlr4yrr162t8.

[22] EVE-NG, "EVE - The Emulated Virtual Environment for Networks, Security and DevOps Professionals," 2021. https://www.eve-ng.net/.

[23] Kali, "The Most Advanced Penetration Testing Distribution," 2021. https://www.kali.org/.

[24] WMware, "Server Virtualisation Software - vSphere," 2021. https://www.vmware.com/uk/products/vsphere.html.