Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021).
IEEE Xplore Part Number: CFP21ONG-ART; 978-0-7381-1183-4

2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) | 978-1-6654-1960-4/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICICV50876.2021.9388412

A Study on Advancement in Honeypot based Network Security Model

Tanmay Sethi
Department of Information Technology, Mukesh Patel School of Technology Management and Engineering
tanmay.sethi47@nmims.edu.in

Rejo Mathew
Department of Information Technology, Mukesh Patel School of Technology Management and Engineering
rejo.mathew@nmims.edu

***Abstract* — Throughout the years, honeypots have been very useful in tracking down attackers and preventing different types of cyber attacks on a very large scale. It's been almost 3 decades since the discover of honeypots and still more than 80% of the companies rely on this system because of intrusion detection features and low false positive rate. But with time, the attackers tend to start discovering loopholes in the system. Hence it is very important to be up to date with the technology when it comes to protecting a computing device from the emerging cyber attacks. Timely advancements in the security model provided by the honeypots helps in a more efficient use of the resource and also leads to better innovations in that field. The following paper reviews different methods of honeypot network and also gives an insight about the problems that those techniques can face along with their solution. Further it also gives the detail about the most preferred solution among all of the listed techniques in the paper.**

Keywords— Honeypot, Intrusion detection system (IDS) , Modern Honey network, SCADA, Square expectation mistake(SPE), TCP-Stack-Fingerprint

I. INTRODUCTION

Honeypots are widely used by cyber security companies with an aim to detect and trap any unsafe attempt of penetrating into the system. There have been a lot of advances in the field of honeypot model as a way of securing servers and other devices. The Modern honeypot network is also used as an Intrusion Detection System(IDS). Government agencies like National ICT Research and training center also use Honeypots as a security model. Honeypot technology has been in use since three decades now but it is still widely used by large companies to protect their confidential data on the server and more than 80% companies rely on honeypots [20].

According to a research done by [19], an unprotected database gets attacked 18 times in a day. A research was conducted by Comparitech security where they deployed a honeypot on their database and recorded that 175 breaches were made in just 1 hour of deployment.

The main reason honeypots are still used is because it gives a basic log of all attackers and deems fit in training the security team. The fact that it is still able to lure the attackers and fool them is the main reason why it is still used. Even after all these years, this model can still lure the hacker and waste his/her time along with logging in the credentials. In order to achieve this goal of luring in attackers, the honeypot system should get advanced with time. This paper covers some of such techniques which make the honeypot up to date in present scenario and efficient enough to prevent cyber attacks

In the section 2 of the paper, all the previous methods and problems are discussed. Section 3 gives a solution of all the problems in the past work. Section 4 gives a feature wise comparison to their advantages and disadvantages. Section 5 concludes the whole paper and explains the best fit solution along with the scope of future work.

II. ISSUES RELATED TO THE EXISTING SOLUTIONS

A. The Honeynet Project

It basically monitors and analyzes the attacks for intrusion detection tools. The main problem with this method is that it can't use emulation but has to use real time systems and application.

B. The DecoyPort System

If an attacker is trying to get in, this system redirects it to the operating honeypot [2]. DecoyPorts are created on the computers so that no real service can be performed on them. All the system queries and services are redirected to the and network load due to the attack can also be controlled through this. The main problem with this high interaction honeypot system is that it increases the possibility of attack

C. PIC Honeypot

It is a high interaction honeypot and ensures a secure network design. In order to implement this, analysis should be done of all the PLCs and the services (HTTP, HTTPS, ISO-TSAP, and SNMP) working in a protected system. These are then integrated in a Linux based Virtualized simulated environment acting as a honeypot. The main disadvantage for this there is no consideration for any physical and network-based interactions with the honeypot (no shell or VPN access).

D. Different Dynamic Honeypot schemes given in [17][18][19]

It follows self adaptive techniques to outwit the attackers. However, the honeypots get fixed at one location once its deployment and configuration is finalized.

E. Context Aware Honeypots

The main feature of this is that it supports interaction with the intruder [5–7]. But it can only be used for deployment of dynamic honeypot in research field which is in an early phase.

III. SOLUTIONS/COUNTERMEASURES

A. Solution 1

- It deploys honeypots dynamically and identifies machines in a network to analyze about its features like the TCP-Stack-Fingerprint [8] , services, uptime, MAC-Address and IP-Address.
- The diagram given below gives an insight about the concept of the system.

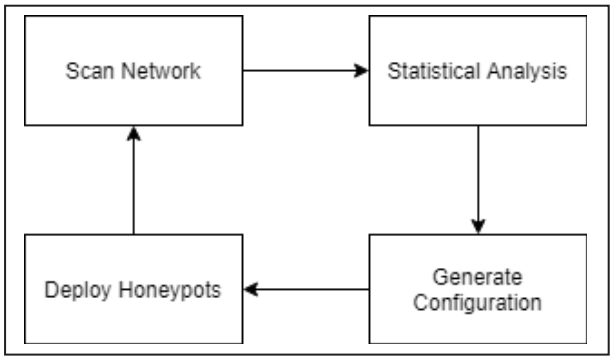

Fig 1: Rough concept of honeypot deployment

- Firstly the network is scanned and the back end database is generated.
- Back end is analyzed in the second step through machine learning in the system.
- As a result, the network gets clustered in groups in accordance to open ports and TCP Stack fingerprint
- The open ports and TCP stack fingerprint are cloned to generate honeypot in the machine within the cluster

- **Implementation:**

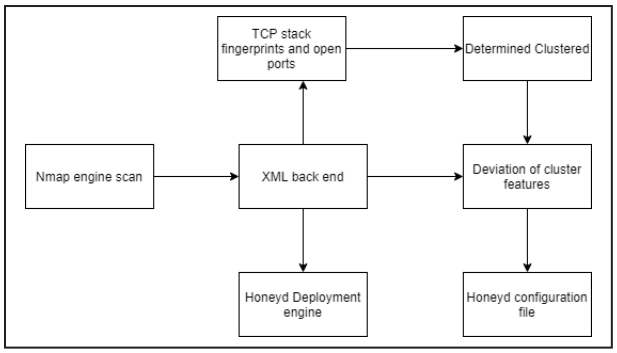

Fig 2: Detailed implementation of the system

This can be further understood by the following chart:

- Scanning engine use- **Nmap.** Nmap is used for network scanning and is used telling the features of algorithm
- **Database Format:** Each network consists of entities. These entities have a unique id and special feature in order to carry out analysis of network after scanning is done
- **Clustering Algorithm – K means:** In order to overcome the drawbacks, some changes have been made. In order for that to happen, the cluster should be dynamic in nature
- **Deployment and Configuration:** Over 65,000 virtual honeypots can be deployed in a network at a time. A text document is used to store the data about configuration so that it can be easily generated by an automated process.

B. Solution 2

- A honeypot acts as a decoy in a network in order to outwit the attacker and collect malware [9].
- The decoy system is made to be just like the system which is being protected in order to lure the attacker into the honeypot, making him think as if he has entered the main system.
- It Gives details about system topology about the attack detection flow.
- The attacker's hardware components and its specification can be found out easily.
- It tells us about the different steps taken by the author to infiltrate and attack on wireless networks. The steps took are: Port scanning, DOS, DDOS attack and brute force attack
- **Modern Honey Network:** It is a management system consisting of different sensors in honeypots which make them act instantly during an attack. The sensors are used to collect attack logs which are then analyzed by MHN. The honeypots involved in this network are:

- **Kippo Honeypots:** An SSH honeypot that logs attacks and all the actions taken by the intruder. It emulates the SSH service and can be used when an attack is made to gain passwords in accordance to SSH service
- **Glastopf Honeypots:** A low involvement honeypot which is used to detect vulnerabilities across web application It outwits the attacker who is planning
- **Dionaea Honeypot:** It traps the tissue attacking malware and obtains its copy so that analysis can be done it.

C. Solution 3

- The third solution presents SIPHON: a Scalable high-Interaction Physical Honeypot [10].
- It is an IoT device that has a lot of tunnels which are used to forward traffic to the wormholes (remote public IP addresses) to the local physical IoT devices.
- This has an architecture is also scalable.
- If there are x physical IoT devices and y wormholes, the number of devices available to the attacker, without repetition can be up to X x Y
- This honeypot can also be implemented in various areas, for instance IP camera honeypot [11] that can be used for home or public surveillance
- **Design Overview:**
  - **Wormholes:** its main role is to make open ports available for public IP over internet. The incoming traffic is either logged or forwarded to the IOT device through forwarding device.
  - **Forwarder:** It re-writes the traffic between Iot device and the wormhole.
  - **Device under Attack:** It is the IOT device which will be under attack. The device should be able to expose a service via TCP and should be able to handle concurrent connections at a single point.
  - **Storage and analysis Unit:** It makes the data ready for offline analysis by collecting traffic records and general logs from the wormholes.

D. Solution 4

- This solution proposes the design of a virtual, high interaction, server-based ICS honeypot [12].
- Virtualization helps in coming up with a cost effective, easily configurable, maintainable and deployable solution.
- High interaction helps in keeping the intruder busy for longer time by running different services.
- It is server based, as the services should not get unrealistic.
- This could be used in research to get to know about different attacks, while plant operators could use the honeypot system to detect specific attacks on their system, or fight the current attacks acting on their system.
- **Honeypot implementation with MiniCPS**:
  - It targets Ethernet/IP based ICS.
  - The figure 3 gives a basic idea about basis of implementation using Ethernet/IP
  - The internet connecting devices are connected as bait.
  - It has a virtual switch which distributes Ethernet/IP traffic in network. It also enables ARP attacks, packet sniffing and other listed malicious commands.

E. Solution 5

- It is a dynamic distributed honeypot based on blockchain [13][14].
- *X* hosts and four services are used to form this system.
- There are two participators: an intruder and the user who is synced in with the real service (i.e., the client is knows the exact location and space of the services)
- X hosts make up a private blockchain, and is called P2P blockchain which is restricted to the public [15].
- **Communication:**
  - The center host (one which mines a block) assigns services to all the other hosts by producing conversion information related to that.
  - These services are carried out through randomly generated algorithm
  - The service numbers and encoding are encrypted by RSA 2048-bit algorithm.
  - The hosts then send the data to the center host privately which is then decrypted to obtain the plain text
  - In the case of 01 encoding, 0 represents starting of honeypot service and 1 represents real service
  - After a comparison, execution is done and the process is ended.
  - The process is streamlined in a way such that if the user logging in is genuine then resources can be shared with him.

IV. EXPERIMENTAL ANALYSIS AND RESULTS

	Solutions				
	Solution 1	***Solution 2***	***Solution 3***	***Solution 4***	***Solution 5***
Level of ineractio n	Low Interacti--on	Low interaction	High interaction	High Interaction	Combines high interaction honeypot with a low interaction honeypot
Nature of deploye ment	Dynamic	Dynamic	Dynamic	Dynamic	Dynamic
Affordab ility	Affordabl e	Affordable	Affordable	Affordable	Affordable
Scalabilit y	Not Scalable	Scalable	Scalable	Not Scalable	Not Scalable
Basis of Solution	TCP	-	IOT	Server based ICS	Blockchain
Method of intruion detection	Nmap is used to scan the intruder	Kippo honeypot interacts with the user on authorisati on	Wormhole firstlogs in the traffic and then tunnels it to the forwarder which then applies a certain way of forwarding	Virtuaizati on and high interaction of honeypot comes in handy	Kippo honeypot interacts with the user on authorizati on
Applicati ons	Large enterprise s	National ICT Training and Research Center (PUSTIKN AS)	IP camera honeypot	Can be used by Plant operators	Can be used by security agency to prevent eavesdropp ing attack, scanning attack and DOS attack

V CONCLUSION

The above paper explained a number methods for implementation of honeypot system. Out of all three solutions, solution 5 seems to be the best fitted solution as it outperforms all the other systems. It also more efficient and reduces the attacking load. Future work should be done on improving the response time of the honeypot system based on the blockchain so that in the case of low attack traffic, it doesn't become inefficient.

REFERENCES

[1] L. Spitzner. The honeynet project: Trapping the hackers. IEEE Security & Privacy, 1(2):15{23, 2003.
[2] The DecoyPort: Redirecting Hackers to Honeypots.Springer Berlin Heidelberg, Sept. 2007.
[3] D. I. Buza, F. Juhász, G. Miru, M. Félegyházi, and T. Holczer. CryPLH: Protecting smart energy systems from targeted attacks with a PLC honeypot. In Proceedings of the Workshop on Smart Grid Security, pages 181–192. Springer,2014.
[4] T. Holczer, M. Félegyházi, and L. Buttyán. The design and implementation of a PLC honeypot for detecting cyber attacks against industrial control systems. https://www.crysys.hu/publications/files/HolczerFB2015CN.pdf,2015.
[5] [4] G. Wagener, R. State, A. Dulaunoy, T. Engel, Heliza: talking dirty to the attackers, Computer Virology (2010).
[6] G. Wagener, R. State, T. Engel, A. Dulaunoy, Adaptive and Self-Configurable Honeypots, 12th IFIP/IEEE International Symposium on Integrated Network Management (2011) 345–352.
[7] A. Pauna, I. Bica, RASSH- Reinforced Adaptive SSH Honeypot, 10th International Conference on Communications (2014).
[8] D. Fraunholz, M. Zimmermann and H. D. Schotten, "An adaptive honeypot configuration, deployment and maintenance strategy," 2017
[9] Wafi, Hibatul & Fiade, Andrew & Hakiem, Nashrul & Bahaweres, Rizal. (2017).Implementation of a modern security systems honeypot Honey Network on wireless networks.
[10] Guarnizo, Juan David, et al. "Siphon: Towards scalable high-interaction physical honeypots." *Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security*. 2017.
[11] Dyn attack 2016. http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.Accessed: 2016-12-06.
[12] Antonioli, D., Agrawal, A., & Tippenhauer, N. O. (2016, October). Towards high-interaction virtual ICS honeypots-in-a-box. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy* (pp. 13-22).
[13] L. Y. Shi, J. Li, X. Liu, and C. F. Jia, ``Research on dynamic array honeypot for collaborative network defense strategy," *J. China Inst. Commun.*vol. 33, no. 11, pp. 159_ 164, Nov. 2012.
[14] R. Sara and D. Ralph, ``Performance analysis of ethereum transactions in private blockchain," in *Proc. 8th IEEE Int. Conf. Softw. Eng. Service Sci.(ICSESS)*, Nov. 2018, pp. 70_74.
[15] Shi, L., Li, Y., Liu, T., Liu, J., Shan, B., & Chen, H. (2019). Dynamic distributed honeypot based on blockchain. *IEEE Access*, *7*, 72234-72246.
[16] https://www.drupal.org/project/usage/honeypot
[17] C. Hecker and B. Hay, ``Automated honeynet deployment for dynamic network environment," in *Proc. 46th Hawaii Int. Conf. Syst. Sci.*, Jan. 2013,pp. 4880_4889.
[18] D. Fraunholz, M. Zimmermann, and H. D. Schotten, ``An adaptive honeypot con_guration, deployment and maintenance strategy," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2017, pp. 53_57.
[19] W. Fan, D. Fern«dez, and Z. Du, ``Versatile virtual honeynet management framework," *IET Inf. Secur.*, vol. 11, no. 1, pp. 38_45, 2016.
[20] Mugunthan, S. R. (2019). SOFT COMPUTING BASED AUTONOMOUS LOW RATE DDOS ATTACK DETECTION AND SECURITY FOR CLOUD COMPUTING. Journal of Soft Computing Paradigm (JSCP), 1(02), 80-90.
[21] Shakya, S. (2019). AN EFFICIENT SECURITY FRAMEWORK FOR DATA MIGRATION IN A CLOUD COMPUTING ENVIRONMENT. Journal of Artificial Intelligence, 1(01), 45-53.