MEDIUM INTERACTION HONEYPOT FOR NETWORK SECURITY TO DETECT CYBER ATTACKS

K. S. Dhanalakshmi
Assistant professor III, Department of ECE. School of Electronics and Electrical Technology.
Kalasalingam Academy of Research and Education, Anand Nagar.
Krishnankoil, Virudhunagar District, (India).
E-mail: k.s.dhanalakshmi@klu.ac.in
ORCID: https://orcid.org/0000-0003-2667-1016

V. BabyShalini
Assistant professor III, Department of IT. School of Computing.
Kalasalingam Academy of Research and Education, Anand Nagar.
Krishnankoil, Virudhunagar District, (India).
E-mail: v.babyshalini@klu.ac.in
ORCID: https://orcid.org/0000-0001-8637-3921

Recepción: 28/11/2019 **Aceptación:** 26/01/2021 **Publicación:** 30/11/2021

Citación sugerida:
Dhanalakshmi, K. S., y BabyShalini, V. (2021). Medium interaction honeypot for network security to detect cyber attacks. *3C Tecnología. Glosas de innovación aplicadas a la pyme, Edición Especial,* (noviembre, 2021), 397-409. https://doi.org/10.17993/3ctecno.2021.specialissue8.397-409

ABSTRACT

A Honeypot is a computer framework that is set up to act as a trap to draw computerized aggressors, and to recognize, divert or focus on attempts to gain unapproved access to information systems. It can distract adversaries from more significant machines on a system give early cautioning about new attack and misuse trends, or permit top to bottom examination of adversaries during and after abuse of a honeypot. Deploying a physical honeypot is frequently time concentrated and expensive as various operating systems require particular hardware and every honeypot requires its own physical framework. To overcome this, a framework of honeypot is made virtually with Medium Interaction by utilizing Kali Linux on Raspberry Pi3. Also, this setup can able to find DoS attack effectively which is created by the attacker.

KEYWORDS

Honeypot, Medium Interaction, DoS attack, Kali Linux on Raspberry Pi3.

https://doi.org/10.17993/3ctecno.2021.specialissue8.397-409

1. INTRODUCTION

The Network security ought to be a high priority while considering a system setup because of the growing threat of hackers endeavoring to infect as many computers possible. Also, the Internet is comprised of a huge number of systems, interconnected without limit. So, the security is crucial in this environment in light of the fact that any authoritative network is accessible from any computers in the world and, hence potentially vulnerable to threats from people who don't require physical access to it.

Honeypot Systems are phony servers or frameworks arrangement to amass data concerning an attacker or gatecrasher into our framework. Today, Honeypots are still in their earliest stages, developed and utilized principally by analysts and security enthusiasts. Honeypot innovation is pushing forward quickly, and, in future honeypots will be difficult to ignore (Pa *et al.*, 2016).

It can fill the growing gaps left by traditional IDS, which experience the ill effects of false positives and a lack of alert intelligence (Kondra *et al.*, 2016). Accordingly, we're going to see much more extensive deployments in the following years. Remember that Honey Pots don't supersede other regular Internet security structures they are an extra system (Bhuyan, Bhattacharyya, & Kalita, 2015) that make sense of how gatecrashers test and try to get to our frameworks systems. The general thought behind is that since a record of the intruder's exercises is kept, we can get understanding into assault procedures to all the more likely guarantee our genuine creation frameworks. This paper initially focused on what is honeypot and reasons why honeypots are essential in network field. We shall then concentrate on how a honeypot can be setup on a system utilizing kali Linux on Raspberry Pi3. Following this we shall then demonstrate some real time simulation of how honeypots have been utilized and what were the results. At long last we shall talk about our future work that is smart honeypot creation in SCADA environment.

2. RELATED WORKS

In the literature, we find extensive studies of detecting the attacker by various methods. Many investigations try to reduce the unauthorized activity. However, sometimes it needs more time to predict the hacker and also low accuracy. In their work, Wang and Jones (2018), use

https://doi.org/10.17993/3ctecno.2021.specialissue8.397-409

a genetic algorithm to finding misbehavior. Here fuzzy membership function is used with vectorized fitness function in GA for efficient intrusion detections. The experimental result shows that the proposed fuzzy vectorized GA performance is better than the vectorized GA and weighted vectorized GA in detecting network attacks for the considered NSL-KDD dataset. In their research, Sadhasivan and Balasubramanian (2017a), use KDD –Dataset as a datamining.

The multiagent based IDA employs the distance and density-based algorithms for cluster formation. The rules formation in either association or sequential manner detects and classifies the attacks to respective agent. Finally, the fuzzy-rules formulation in MAIDS predicts the intrusion type. In the paper of Meoch (1999), the author improves the IDS and use the multiagent concept with multilevel intrusion detection system. Here we store the attack type is matched with this database then it detects the intrusion. The main advantage is it need less time to detect the intruder. In their work, Lee and Huang (2013), IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems) increasingly use SOM (Self-Organizing Map). Here the total accuracy is 93%. Here the web information is uncertainty.

In their work, Armstrong, Korah, and Salivahanan (2018), can speed up the task execution efficiency, and improve the throughput of the system. Sometime it is Difficult to find the attacker. In the work of Armstrong *et al.* (2018), intrusion detection is the fundamental research region in field of system security. It includes the observing of the occasions happening in a PC framework and its system. Data mining is one of the advancements connected to ID to develop another example from the gigantic system information just as to decrease the strain of the manual assemblage of the interruption designs. Remembering, data mining techniques are drilled altogether ID and aversion. This article surveys the present condition of data mining technique with ID in a word and features its preferred position and drawback

3. PROPOSED METHOD

In this paper the Medium Interaction honeypot is created by using ARM based Kali Linux (With Raspberry Pi). Figure 1 indicates that the representation of flow diagram of our work.

https://doi.org/10.17993/3ctecno.2021.specialissue8.397-409

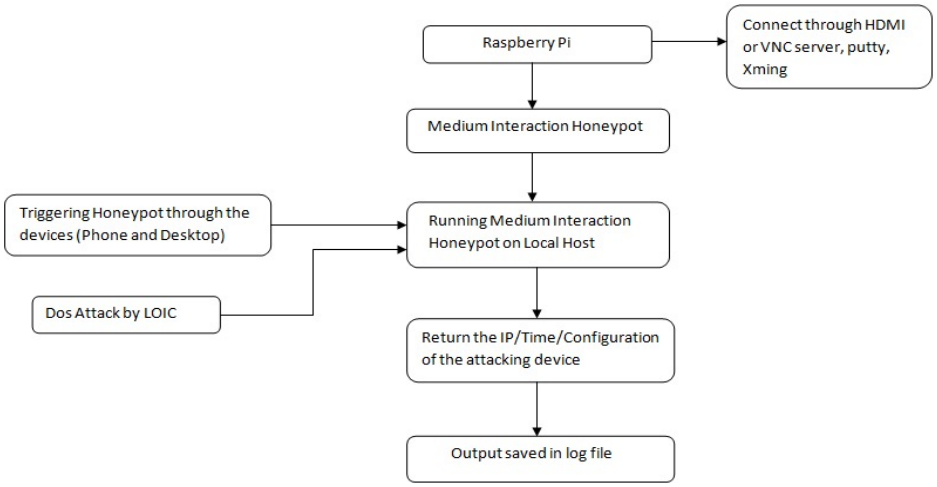

Figure 1. Idea of the work.
Source: own elaboration.

3.1. MEDIUM INTERACTION HONEYPOT

Interaction based honeypot implies how much the honeypot making an interaction with the attacker. The Low Interaction honeypot is easy to configure and just great at catching Known attack patterns, however it is useless at interacting or finding obscure attack signatures. So, the medium interaction Honeypot is made which will rise above the drawbacks of Low Interaction Honeypot.

3.2. ARM BASED KALI LINUX

Kali Linux is a standout amongst the most well-known penetration testing stages utilized by security experts, hackers, programmers, and researchers around the globe for security and defenselessness evaluation attack research and risk testing. It offers a wide assortment of prominent open-source tool that can be utilized in all aspects of penetration testing. Kali Linux has developed from back track 5 R3 into a model of an entire desktop working framework. The Raspberry pi is an extremely low-cost computer that attachments into a monitor utilizing HDMI (High-Definition Multimedia interface) and utilizations our own USB console and mouse. It gives an environment to learn processing and programming.

https://doi.org/10.17993/3ctecno.2021.specialissue8.397-409

Figure 2. Experimental Setup in Real time.
Source: own elaboration.

Figure 2 shows the Real time experimental setup. Here Raspberry Pi is connected through HDMI and the Medium Interaction Honeypot framework is created and it will be detecting the IP triggering given by various devices (Phone, Laptop) as well as DoS attack given by LOIC (Low Orbit Ion Canon).

4. SIMULATION OUTPUTS

The proposed idea is tested in real time with various attacking devices with Dynamic IP addresses. When an Intruder trying to block the specific IP address by hitting the particular IP or create a attack, the Medium Interaction honeypot will capture the specific activities. The honeypot act as a production or research honeypots depending on their requirement while implementation.

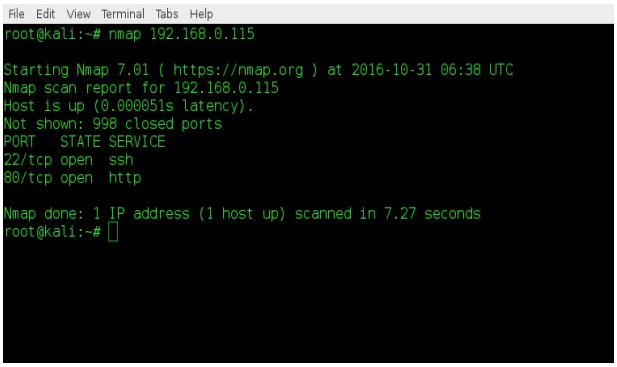

Figure 3. IP scanning using Nmap command.
Source: own elaboration.

https://doi.org/10.17993/3ctecno.2021.specialissue8.397-409

Initially the IP scanning process take place using the nmap command that will be shown by the Figure 3. After completing the scanning process honeypot will produce the entire details like type of attacking device, IP address of the attacking device, time of attack and the configuration.

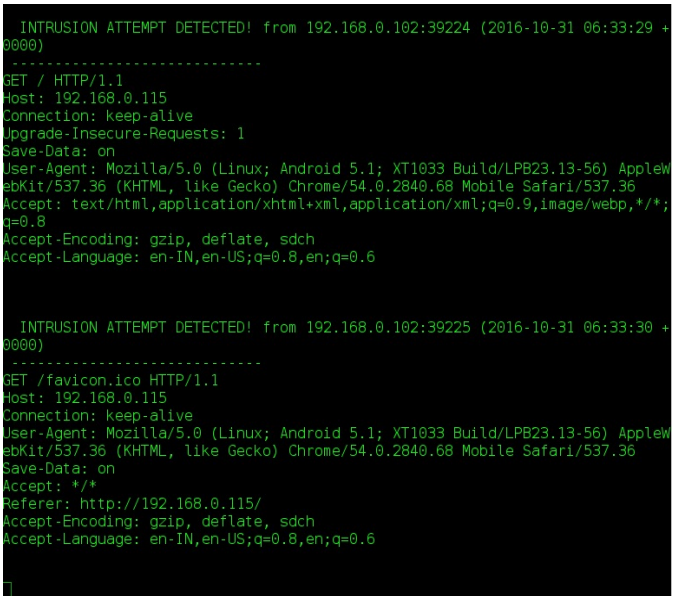

Figure 4. Intrusion created by the laptop is detected by the Honeypot.
Source: own elaboration.

Here the Intrusion is given by both Laptop and Mobile Phone via dynamic IP address. The action of Medium Interaction Honeypot is simulated after the intrusion and the result is displayed in Figures 4 and 5. The attack would make a fruitful TCP connection and possibly exchange its payload. This payload would then be spared locally on the honeypot, which can be further broke down by the admin, who can survey the thread.

https://doi.org/10.17993/3ctecno.2021.specialissue8.397-409

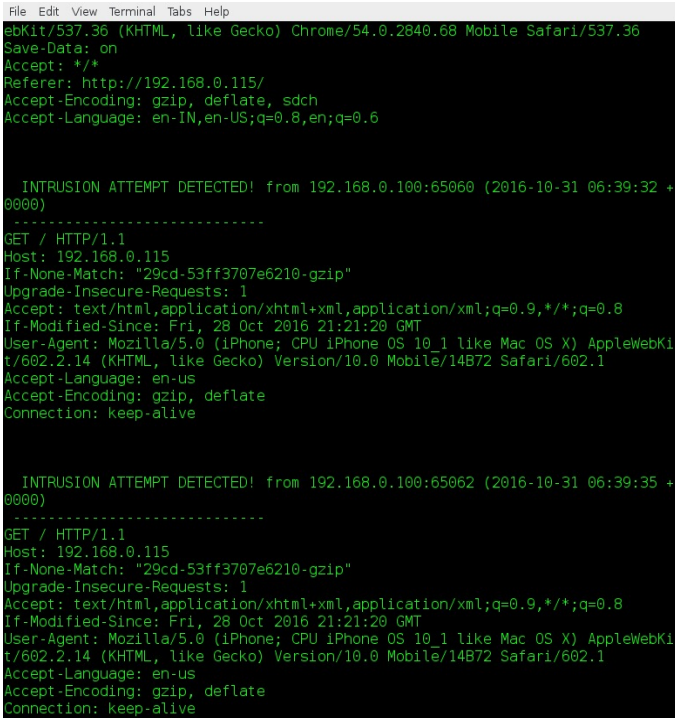

Figure 5. Intrusion created using mobile is detected by the Honeypot.
Source: own elaboration.

The DoS (Denial of Service) attack is one of the all the more intense hacks, able to do totally bringing a server down. Thusly, the server won't have the ability to deal with the requesting of considerable customers. A LOIC (Low Orbit Ion Cannon) is a champion among the best DoS assaulting apparatuses uninhibitedly open. LOIC plays out a DoS attack (or when utilized by numerous people, a DDoS attack) on an objective site by flooding the server with TCP or UDP packets with the expectation of disturbing the administration of a specific host.

https://doi.org/10.17993/3ctecno.2021.specialissue8.397-409

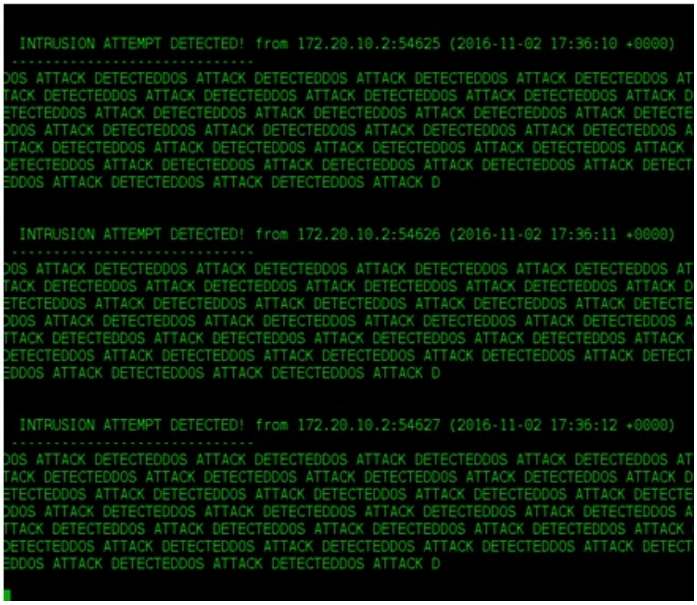

Figure 6. Detection of DoS attack by the Honeypot.
Source: own elaboration.

5. CONCLUSIONS

Like all technologies, honeypots have their drawbacks, the greatest one being their limited field of view. Honeypots capture only activity that's directed against them and will miss attacks against other systems. For that reason, security experts don't recommend that these systems replace existing security technologies. Instead, they see honeypots as a complementary technology to network- and host-based intrusion protection. The advantages that honeypots bring to intrusion-protection solutions are hard to ignore, especially now as production honeypots are beginning to be deployed. In time, as deployments proliferate, honeypots could become an essential ingredient in an enterprise-level security operation.

We have implemented the Medium Interaction Honeypot and the proposed honeypot will effectively taking action while finding the intrusion. The intrusion was given by the various devices and the response given by the honeypot was presented and analyzed. Anyway, this framework is now implemented for the small network. In future we have planned to implement this work for large-scale real-time automation industries for security in SCADA environment.

https://doi.org/10.17993/3ctecno.2021.specialissue8.397-409

ACKNOWLEDGEMENT

We thank the Department of Electronics and Communication Engineering, School of Electronics and Electrical Technology of Kalasalingam Academy of Research and Education, Tamil Nadu, India for permitting to use the computational facilities available in Centre for Research in Signal Processing and VLSI Design which was setup with the support of the Department of Science and Technology (DST), New Delhi under FIST Program.

REFERENCES

Armstrong, J. J., Korah, R., & Salivahanan, S. (2018). Efficient String Matching FPGA for speed up Network Intrusion Detection. *Applied Mathematics & Information Sciences: an International Journal, 12*(2), 397-404. http://www.naturalspublishing.com/files/published/u40jti0ukf6096.pdf

Baykara, M., & Firat, R. D. (2015). A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems. *International Journal of Computer Networks and Applications, 2*(5), 203-211. https://www.ijcna.org/Manuscripts/Volume-2/Issue-5/Vol-2-issue-5-M-01.pdf

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). Towards Generating Real-life Datasets for Network Intrusion Detection. *International Journal of Network Security, 17*(6), 683-701. http://ijns.jalaxy.com.tw/contents/ijns-v17-n6/ijns-2015-v17-n6-p683-701.pdf

Chalamasetty, G. K., Mandal, P., & Tseng, T.-L. (2016). Secure SCADA communication network for detecting and preventing cyber-attacks on power systems. In *2016 Clemson University Power Systems Conference (PSC)*, 1-7. https://doi.org/10.1109/PSC.2016.7462865

Dhanalakshmi, K. S., & Kannapiran, B. (2017). Analysis of KDD CUP Dataset Using Multi-Agent Methodology with Effective Fuzzy Based Intrusion Detection System. *Journal of Applied Security Research, 12*(3), 424-439. https://doi.org/10.1080/19361610.2017.1315760

Jyothi, V., Addepalli, S. K., & Karri, R. (2018). DPFEE: A High Performance Scalable Pre-Processor for Network Security Systems. *IEEE Transactions on Multi-Scale Computing Systems, 4*(1), 55-68. https://doi.org/10.1109/TMSCS.2017.2765324

Kabiri, P., & Ghorbani, A. A. (2005). Research on intrusion detection and response: A survey. *International Journal of Network Security, 1*(2), 84-102. https://www.researchgate.net/publication/45681663_Research_on_Intrusion_Detection_and_Response_A_Survey

Kondra, J. R., Bharti, S. K., Mishra, S. K., & Babu, K. S. (2016). Honeypot-based intrusion detection system: A performance analysis. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 3947-3951. https://ieeexplore.ieee.org/document/7724682

Lee, T.-H., & Huang, N.-L. (2013). A pattern-matching scheme with high throughput performance and low memory requirement. *IEEE/ACM Transactions on Networking (TON), 21*(4), 1104-1116. https://dl.acm.org/doi/10.1109/TNET.2012.2224881

Luo, B., & Sun, Z. (2015). Research and Implementation of a Network Secure System Based on Honeypots. *Proceedings of the 2nd International Conference on Civil, Materials and Environmental Sciences*, 224-227. https://doi.org/10.2991/cmes-15.2015.64

Meoch, R. (1999). Snort-Lightweight intrusion detection for network. *Proceedings of the 13th System Administration*, Vol. 238. https://dl.acm.org/doi/10.5555/1039834.1039864

Pa, Y. M. P., Yoshioka, K., Matsumoto, T., Kasama, T., & Rossow, C. (2016). IoTPOT: A Novel Honeypot for Revealing Current IoT Threats. *Journal of information processing, 24*(3), 522-533. https://doi.org/10.2197/ipsjjip.24.522

Sadhasivan, D. K., & Balasubramanian, K. (2017a). A fusion of multiagent functionalities for effective intrusion detection system. *Security and Communication Networks, Article ID 6216078*. https://doi.org/10.1155/2017/6216078

Sadhasivan, D. K., & Balasubramanian, K. (2017b). A novel LWCSO-PKM-based feature optimization and classification of attack types in SCADA network. *Arabian*

Journal for Science and Engineering, 42(8), 3435-3449. https://doi.org/10.1007/s13369-017-2524-0

Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access, 4, 1375*-1384. https://doi.org/10.1109/ACCESS.2016.2549047

Selvaraj, R., Kuthadi, V. M., & Marwala, T. (2016). Honey Pot: A Major Technique for Intrusion Detection. In Satapathy, S., Raju, K., Mandal, J., & Bhateja, V. (eds.) *Proceedings of the Second International Conference on Computer and Communication Technologies*. Advances in Intelligent Systems and Computing, vol 380. Springer, New Delhi. https://doi.org/10.1007/978-81-322-2523-2_7

Simoes, P., Cruz, T. J., Proença, J., & Monteiro, E. (2015). Specialized Honeypots for SCADA Systems. In Lehto, M., & Neittaanmäki, P. (eds.) *Cyber Security: Analytics, Technology and Automation*, vol 78, Chapter: Part IV, Chapter 3. Springer International Publishing. https://doi.org/10.1007/978-3-319-18302-2

Wang, L., & Jones, R. (2018). Big Data Analytics of Network Traffic and Attacks. In *NAECON 2018-IEEE National Aerospace and Electronics Conference*. https://ieeexplore.ieee.org/document/8556802

Wang, W., Liu, J., Pitsilis, G., & Zhang, X. (2018). Abstracting massive data for lightweight intrusion detection in computer networks. *Information Sciences, 433-434*, 417-430. https://doi.org/10.1016/j.ins.2016.10.023

Zhang, Z., Li, J., Manikopoulos, C. N., Jorgenson, J., & Ucles, J. (2001). HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.67.857&rep=rep1&type=pdf

https://doi.org/10.17993/3ctecno.2021.specialissue8.397-409