International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 06 | June 2021 www.irjet.net p-ISSN: 2395-0072

Learning Automata for Adaptive Honeypot Detection using Machine Learning

Prof. Renuka B S [1], Abhishek G[2]

[1]*Associate Professor, Dept. of Electronics & Communication, JSS Science and Technology University, Mysuru, Karnataka, India.*

[2]*PG student, Dept. of Electronics and Engineering, JSS Science and Technology University, Mysuru, Karnataka, India.*

Abstract - This paper describes Computerized utilize honeypot identifying instruments inside its code. When honeypot usefulness has been uncovered, malware will stop the endeavored bargain. Resulting malware variations utilize comparative methods to dodge recognition by known honeypots. This diminishes the expected size of a caught dataset and resulting examination. Assaults on the web continue expanding and it makes hurt our security framework. To limit this danger, it is important to have a security framework that can recognize zero-day assaults and square them. The investigation of the traffic that movements in the organization are a basic errand. Traffic investigation on the organization is finished by introducing different organization interruption discovery (NID) gadgets. One of the essential gadgets for recognizing network interruptions is a Honeypot. Honeypots connect with the aggressor and gather the information which can be broke down to recover data in regards to the assaults and assailant in the organization. Honeypots are security assets that are focused on by the aggressor and produce information logs of the assaults. Honeypots give applicable information in a little amount with the goal that security scientists could without much of a stretch comprehend and the examination of the information gets achievable. This task presents discoveries on the organization of a honeypot utilizing support learning, to cover usefulness. The versatile honeypot learns the best reactions to conquer starting location endeavors by carrying out a prize capacity fully intent on augmenting assailant order changes. The undertaking shows that the honeypot rapidly distinguishes the best reaction to beat starting location and accordingly builds assault order changes. It likewise inspects the construction of a caught botnet and graphs the learning advancement of the honeypot for dull mechanized malware. At long last, it recommends changes to a current scientific categorization overseeing honeypot advancement, in light of the learning development of the versatile honeypot.

Key Words: Honeypot, Honeynet, Kojoney, NID gadgets.

1.INTRODUCTION

A honeynet is an arrangement of honeypots that are set up to attract anyway numerous attackers as would be reasonable to get some answers concerning their models, systems, and practices. Regardless, existing honeypots experience the evil impacts of an arrangement of fingerprinting strategies, and the current honeynet designing doesn't totally utilize the features of living honeypots in light of its coarse-grained data control frameworks. To address these challenges, we propose an SDN-based sharp honeynet called Honey pot. Nectar pot utilizes the rich programmability of SDN to sidestep attackers' disclosure instruments and engages fine-grained data control for honeynet. To do this, Honey pot simultaneously sets up a different relationship with a lot of honeypots and picks the best relationship with awakening aggressors to remain related. In this endeavor, we present the Honey pot designing and a depiction of its middle fragments. Honeypots, as a sort of electronic draws, are attempted to deliberately open powerless resources for aggressors to help to test and manhandling. Since the basic objective of honey□pots is to get some answers concerning aggressors' practices and catch new sorts of malware, honeypots don't have to complete all functionalities of a creation system. Accordingly, honeypots regularly duplicate or replicate certain systems and organizations to reduce the computational and upkeep cost. Another honeypot called Kojoney, which furthermore offers an SSH organization, just necessities a barely unprecedented area procedure, since it returns the timestamp when Kojoney was presented. Using such acknowledgment strategies, aggressors can without a doubt separate honeypots and act particularly sometime later. Thusly, methodologies that hold aggressors back from distinguishing the presence of duplicated structures and organizations are essential in building incredible nectar pots. In the current framework Hybrid honeypots normally contain different fronts closes (low-association honeypots) that can mimic huge number of IP to draw in aggressors and back-closes (high-collaboration honeypots) which can inter□face profoundly with the assailant to get nitty gritty assault data. Hence, we could examine more important traffic to fortify the creation organization. Be that as it may, the customary half breed nectar pot design experiences issues in framework stream control, and the actual machine arrangement is awkward. Even with a changing organization climate, it is difficult to make designated acclimations to arrange traffic changes to acquire powerful data. The full paper is organized as follows: Section II describes the related work which signifies each work in the context of its contribution for understanding the research problem,

Section III deals with the system practicability. Section IV shows the experimental results of the designed system and Section V concludes the paper.

2. RELATED WORK

Assaults on the web continue expanding and it makes hurt our security framework. To limit this danger, it is important to have a security framework that can distinguish zero-day assaults and square them. "Honeypot is the proactive safeguard innovation, where assets set in an organization with the mean to notice and catch new assaults". This paper proposes a honeypot-based model for interruption location framework (IDS) to acquire the best valuable information about the assailant. The capacity and the constraints of Honeypots were tried and parts of it that should be improved were recognized. Later on, we mean to utilize this pattern for early counteraction with the goal that pre-emptive move is made before any unforeseen mischief to our security framework.2 Malware is one of the dangers to data security that keeps on expanding. In 2014 almost 6,000,000 new malwares was recorded. The most elevated number of malwares is in Trojan pony malware while in Adware malware is the most altogether expanded malware. Security framework gadgets, for example, antivirus, firewall, and IDS signature-based are considered to neglect to recognize malware. This happens due to the quick spread of PC malware and the expanding number of marks. Other than signature-based security frameworks it is hard to recognize new strategies, infections or worms utilized by assailants. One other option in recognizing malware is to utilize honeypot with AI. Honeypot can be utilized as a snare for bundles that are suspected while AI can recognize malware by grouping classes. Choice Tree and Support Vector Machine (SVM) are utilized as arrangement calculations. In this paper, we propose structural plan as an answer for distinguish malware. We introduced the design proposition and disclosed the exploratory strategy to be utilized.

3. SYSTEM PRACTICABILITY

This Project aims to redirect malevolent traffic from significant frameworks and get early admonition of a current assault before basic frameworks are hit and also to accumulate data about the aggressor and the assault strategies. Regardless, existing honeypots experience the evil impacts of a collection of fingerprinting strategies, and the current honeynet designing doesn't totally utilize features of living honeypots in view of its coarse-grained data control segments. To address these challenges, we propose a SDN-based brilliant honeynet called Honey pot. Nectar pot utilizes the rich programmability of SDN to circumvent attackers' disclosure segments and enables fine-grained data control for honeynet. To do this, Honey pot meanwhile sets up various relationship with a lot of honeypots and picks the best relationship with rousing aggressors to remain related. In this endeavor, we present the Honey pot plan and a portrayal of its middle fragments.

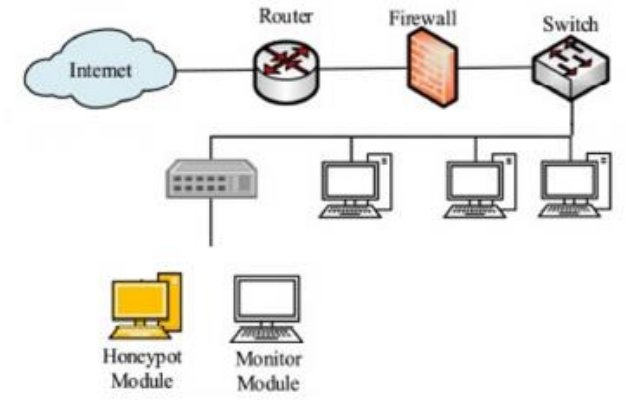

Fig-1: Block diagram of Honeypot network

A.Python

Python is a deciphered, significant level, broadly useful programming language. Made by Guido van Rossum and first delivered in 1991, Python's plan reasoning accentuates code comprehensibility with its prominent utilization of critical whitespace. Its language builds and item situated methodology expect to assist software engineers with composing, consistent code for little and enormous scope projects. Python is progressively composed and trash gathered. It upholds numerous programming standards, including procedural, object-situated, and practical programming. Python is frequently portrayed as a "batteries included" language because of its extensive standard library. Python was imagined in the last part of the 1980s as a replacement to the ABC language. Python 2.0, delivered in 2000, presented highlights like rundown understandings and a trash assortment framework equipped for gathering reference cycles. Python 3.o, delivered in 2oo8, was a significant correction of the language that isn't totally in reverse viable, and much Python 2 code doesn't run unmodified on Python 3. The Python 2 language, for example Python 2.7.x, was formally ceased on January 1, 2020 (first made arrangements for 2o15) after which security patches and different enhancements won't be delivered for it. With Python 2's finish of-life, just Python 3.5.x and later are upheld. Python mediators are accessible for some working frame□works. A worldwide local area of software engineers creates and looks after CPython, an open-source reference execution. A non-benefit association, the Python Software Foundation, oversees and coordinates assets for Python and CPython improvement.

Fig-2: PYTHON

B. PyCharm

PyCharm is utilized in PC programming with the assistance of an incorporated development climate (IDE), explicitly for the Python language. It gives code examination, a graphica1 debugger, and coordinated unit analyzer, combination with variant control frameworks (VCSes).

C. Numpy

NumPy is a library for the Python programming language, adding support for huge, multi-dimensional clusters and grids, alongside an enormous assortment of undeniable level numerical capacities to work on these arrays. The progenitor of NumPy, Numeric, was initially made by Jim Hugunin with commitments from a few different designers. NumPy is open-source programming and has numerous supporters.3 D. Pandas pandas is a product library composed for the Python programming language for information control and examination. Specifically, it offers information constructions and tasks for controlling mathematical tables and time arrangement. It is free programming delivered under the three-condition BSD permit. The name is gotten from the expression "board information", an econometrics term for informational indexes that incorporate perceptions throughout different time spans for similar people. Its name is a play on the expression "Python information examination" itself. Wes McKinney began building what might become pandas at AQR Capital while he was an analyst there from 2007 to 2010.

E. NetworkX

NetworkX is a Python bundle for the creation, control, and investigation of the construction, elements, and elements of complex organizations. With NetworkX you can load and store networks in norm and nonstandard information designs, produce numerous kinds of arbitrary and exemplary organizations, examine network structure, assemble network models, plan new organization calculations, draw organizations, and considerably more.

4. RESULT

Honeypots give applicable information in a little amount with the goal that security scientists could without much of a stretch comprehend and the examination of the information gets achievable.

This task presents discoveries on the organization of a honeypot utilizing support learning, to cover usefulness. The versatile honeypot learns the best reactions to conquer starting location endeavors by carrying out a prize capacity fully intent on augmenting assailant order changes.

The undertaking shows that the honeypot rapidly distinguishes the best reaction to beat starting location and accordingly builds assault order changes.

It likewise inspects the construction of a caught botnet and graphs the learning advancement of the honeypot for dull mechanized malware. At long last, it recommends changes to a current scientific categorization overseeing honeypot advancement, in light of the learning development of the versatile honeypot.

This undertaking proposes another engineering dependent on SDN applied to the half and half honeypot framework, joined with the qualities of high and low intuitive honeypots for network geography reenactment and assault traffic movement. The framework can reproduce a huge and sensible organization to draw in assailants, and divert undeniable level assaults to a high-connection honeypot for assault catch and further investigation. The SDN regulator gives network geography recreation in the cross breed nectar organization and gives high-accuracy information control in the whole assault traffic movement, which improves the inadequacies in the organization mocking innovation and streams control innovation in the customary nectar organization. At last, we set up the exploratory climate on the mininet and checked the system we proposed. The test outcomes show that the framework is more keen and the traffic relocation is more secretive.

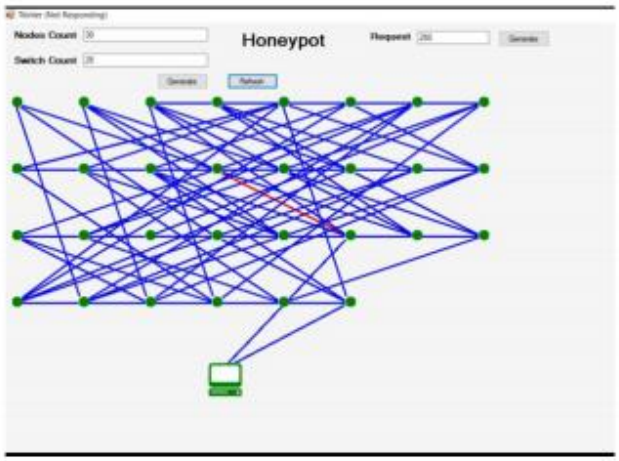

Fig-3: Nodes Requests Connection

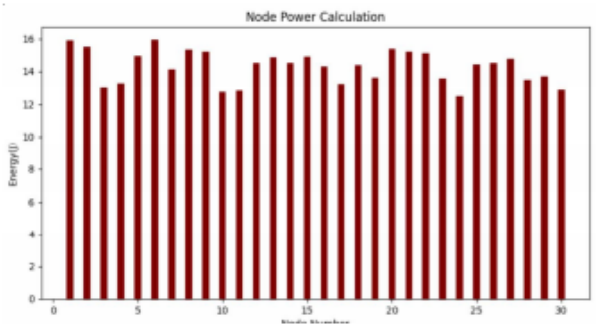

Fig-4: Node to Node Power Calculation

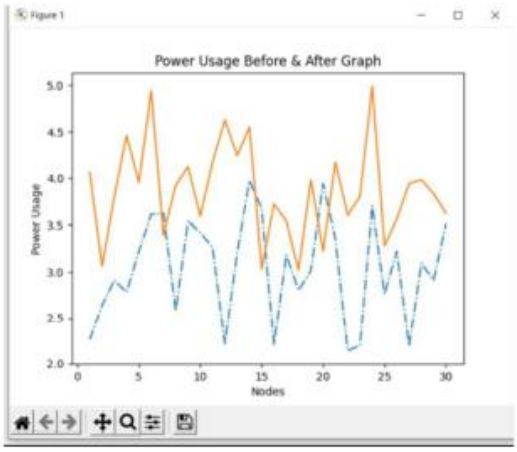

Fig-5: Power Usage

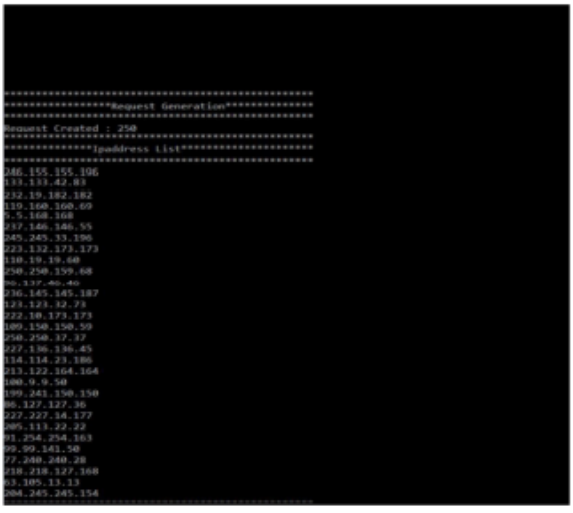

Fig-6: Request Creation

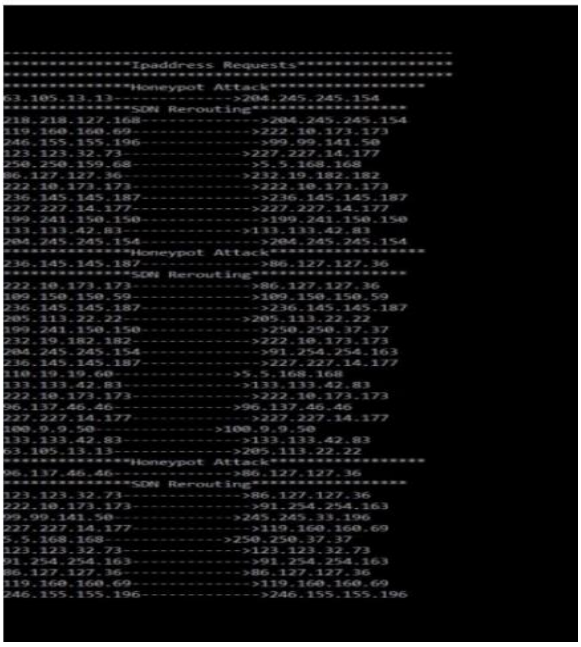

Fig-7: Attack Detection and Rerouting

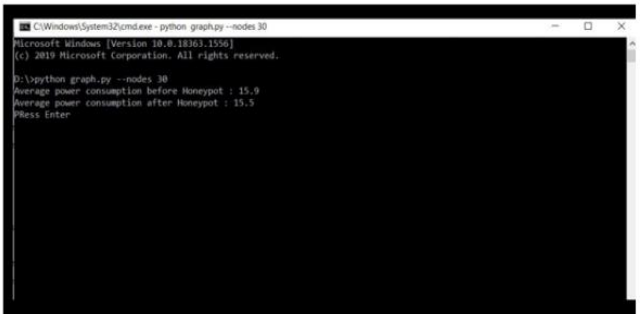

Fig-8: Power Consumption Comparison

5. CONCLUSIONS

The proposed system consists of one of the essential gadgets for recognizing network interruptions is a Honeypot. Honeypots connect with the aggressor and gather the information which can be broke down to recover data in regards to the assaults and assailant in the organization. Honeypots are security assets that are focused on by the aggressor and produce information logs of the assaults.

REFERENCES

[1] Janardhan Reddy Kondra, Santosh Kumar Bharti, Sambit Kumar Mishra, Korra Sathya Babu, Honeypot-based intrusion detection system: A performance analysis, 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom),2016.

[2] Zhang Li-juan, Honeypot-based defense system research and design, China National Digital Switching System Engineering and Technological Research Center, Zhengzhou, Henan,China,2009.

[3] Iik Muhamad Malik Matin, Budi Rahardjo, Malware Detection Using Honeypot and Machine Learning, School of

Electrical Engineering and Informatics, Bandung Institute of Technology, Bandung, Indonesia, 2019.
[4] Neeraj Bhagat , Bhavna Arora, Intrusion Detection Using Honeypots, : 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2018.
[5] Poorvika Singh Negi, Aditya Garg, Roshan Lal, Intrusion Detection and Prevention using Honeypot Network for Cloud Security, 2020 10th International Conference on Cloud Computing, Data Science Engineering 2020.
[6] Li Li, Hua Sun, Zhenyu Zhang, The research and design of honeypot system applied in the LAN security, 2011.
[7] Liu Dongxia, Zhang Yongbo, An Intrusion Detection System Based on Honeypot Technology, 2012 International Conference on Computer Science and Electronics Engineering, 2012.
[8] Abdallah Ghourabi, Tarek Abbes, Adel Bouhoula, Design and implementation of Web Service honeypot, SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks, 2011.
[9] R. McGrew, Experiences with Honeypot Systems: Development, Deployment, and Analysis, 2006
[10] S. Yeldi; S. Gupta; T. Ganacharya; S. Doshi, Enhancing network intrusion detection system with honeypot, 2004.

BIOGRAPHIES

Prof. Renuka B S.
Associate Professor, Dept. of E&C,
JSSSTU, Mysuru.

Abhishek G
M.Tech, Networking and Internet engineering.
Dept. of E&C, JSSSTU, Mysuru.