International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 3 March 2020

Development, Deployment, and Analysis of Honeypot Framework to Improve the Anonymous Network

M. Suresh[1] , R. Brainard Samuel[2]

[1]Assistant Professor, [1,2]Department of Information Technology,
Manakula Vinayagar Institute of Technology, Pondicherry, India
[1]sureshit@mvit.edu.in, [2]brainardjude7@gmail.com

Abstract: Honey pots are intended to trap the assailant with the motivation behind researching its malignant conduct. Attributable to the expanding assortment and modernity of digital assaults, how to catch excellent assault information has turn into a test in the setting of honeypot region. Every honeypots, which mean a huge enhancement in reasonableness, counteract ant, and secrecy, are important to handle the issue. In this article, we intend a novel honeypot design named Honey DOC to help all round honey pot structure and usage. Our Honey DOC engineering unmistakably recognizes three fundamental autonomous and communitarian elements, Distract, Captor, and Orchestrator. In view of the proficient engineering, a product characterized organizing empowered honeypot framework is structured, which contribute a elevated programmability for in fact supporting the highlights for catching great information. A confirmation-of-idea framework is executed to approve its practicality and viability. The test consequences demonstrate the advantages by utilizing the anticipated design thought about with the past honey pot arrangements.

Keywords: Honey pots, DOC engineering

1. INTRODUCTION

PC frameworks over the globe are looked with different security dangers because of programming imperfections and setup mistakes. The results can influence people what's more, associations at basic levels from security exposures to money related misfortunes. Likewise, the difficult to recognize zero-day assaults are getting progressively various and modern, for example there was an expansion of 7 % in the quantity of zero day vulnerabilities recorded in 2017, and 27 % of the 140 focused on assault bunches that Symantec paths have been recognized to utilize zero-day exposed anytime, which were appeared by Symantec 2018's ISTR description. Additionally, digital dangers are frequently went with malignant thought processes, slit within management and secretive frameworks to handicap the armed forces, power supporting advancement, impact the money related field, and harm the administration areas of financial aspects. Such digital surveillance, fighting and fear based oppression have incited extensive alert. To lessen the hazard, an assortment of safety efforts are given, for example firewall, interruption location framework (IDS), and interruption counteractive action framework (IPS). Not at all like these devices mostly being used to forestall assaulting, a honeypot is a particular security office that expects to permit being assaulted for the reason of examining the making of the programmer network by implies of publicizing/ uncovering its data frameworks asset to baitun approved and unlawful access [5]. Other than the caught information amount, the information quality is a much increasingly note worthy viewpoint, which will incredibly affect the assault analysis. With respect to the assortment of assault varieties [6] and the multifaceted nature of assault situations [7], the various- aspects criteria on basis of assault reporting and legal sciences are engaging [8]. For instance, a commonplace DDoS assault receives a great deal of traded off hosts to dispatch simultaneous admittance to the objective server that will result in a DOS; a port-check assault can utilize just one assault have however can include an enormous number of unfortunate assault has, in any case, it does little damage to the people in question; a sort of cushion flood assault can enable the foe to force an entry within injured individual host by abusing the unguarded, which will be hurtful in light of the fact that the aggressor can get to the unfortunate casualty's information and indeed, still can organize the unfortunate casualty to complete more assault; a malicious can stretch on the Internet and taint every one of the people in question, which may cause a disaster universally, for example the WannaCryransom ware [9].

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 3 March 2020

So the test is that a honeypot framework ought to be prepared to do effectively encouraging the enemy with the fitting asset relying upon the assault type for the reason for catching great information. Notwithstanding, most honey pots are just inactively accepting assault information [10], and all the more correctly, they come up short on a reasonableness for completely recognizing and recognizing the different assault information and situations. In spite of various proposition giving a few information control (honey wall [11], honeybrid passage [12], honey proxy [13]) and asset chain of command (crossover honey pots [14]–[16]) so as to address the issue, they are simply case-by-case and uneven arrangements. Moreover, a few countermeasures, for example dynamic organization [17], fascinating traffic redirection, and uninteresting traffic decrease and so on are exceptionally valuable to upgrade the information quality. Be that as it may, current honeypots frequently either overlook giving countermeasures or on the other hand scarcely offer basic ones. Plus, the control on the assault stream and the honeypot assets ought to be stealthy and imperceptible to the foe, generally the further information catch will fall flat. In this manner, a sort of productive honeypot framework, whereby the assault exercises can be delicately grouped and handled in fine-grained ways, and afterward devoured by the unperceived honey pot asset with suitable countermeasures is profoundly required. By and by, the current honeypot frameworks are not ready to give this sort of breadth, on the grounds that there is an absence of engineering that can encourage the inside and out honeypot structure. A two bit honeypot component has been recognized, bait and captor, which can form the honey pot framework asset basically, however the existing honey pot designs regularly give less consideration on the captor, which significantly confines the probability of upgrading the top notch information catch (see the accompanying case 1). Take the angling trap as a representation of honeypots:

Case 1: the snare with lure can get gullible and ravenous fish (like content kiddies), yet presumably will neglect to catch modern fish (like propelled programmers);

Case 2: separate the trap from the snare, and put it into a net, which will be progressively secret, and furthermore will have higher fish catch productivity. When the honeypot framework is separated, the engineering regularly needs an orchestrator to empower them to participate. In this way, this exploration work's goal is to propose a productive honeypot engineering that can organize the two fundamental foundations in order to empower the inside and out honeypot framework configuration to fulfill the reasonableness, counter measure and stealth for different necessities to catch high quality assault information. The commitments of this paper can be outlined as pursues.

An effective honeypot design, to be specific Honey DOC**,** comprising of three modules, for example Distraction, Orchestrator and Captor, is proposed to organize them to empower all-round plan with the end goal of top notch assault information catch.

ASDN-empowered honeypot framework is structured upon the proposed engineering. SDN's programmability and isolated planes completely fulfills the prerequisite of encouraging the three critical highlights, for example reasonableness, counter measure what's more, stealth, and makes the framework extendable too with the goal that it is easy to grow new capacities and coordinate outside outsider parts.

A Proof-of-Concept framework is actualized regarding the SDN-empowered honeypot plan, which is utilized to approve the proposed honeypot design, and furthermore, a few tests are led for assessing the highlights of the model.

2. EXISTING WORK

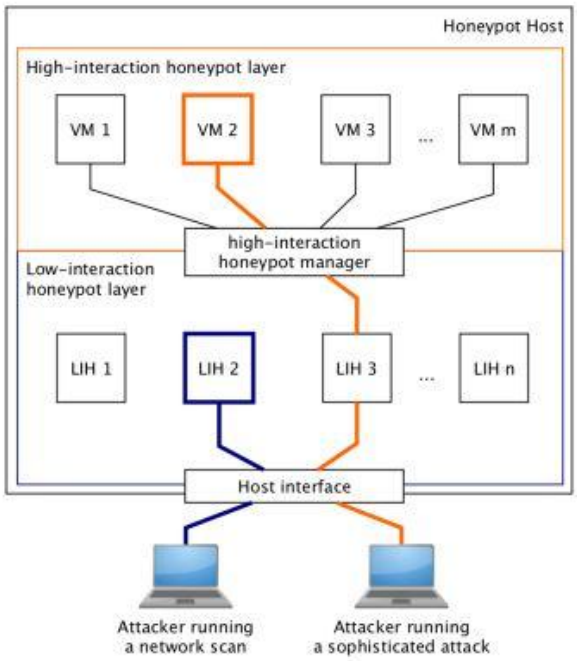
This segment surveys the traditional and SDN-empowered honey pot designs. In the accompanying substance, the abbreviations, LIH, MIH and HIH represent low-collaboration, medium-communication and high interaction honey pot individually. The Honeypot Project proposed a progression of physical honeynet designs including Gen I, II, III which were broadly utilized by associations. For instance, Georgia Tech applied the Gen I honeynet design to oversee traded off PCs over the grounds systems. From that point, the virtualization innovation was acquainted with encourage the virtual honey net arrangement, which makes one physical have running different visitors. In any case, this customary honeynet engineering comes up short on the capacity of huge scale organization. In 2006, a half breed honey pot system was proposed [14], which coordinated the renowned low-connection virtual honeypot system with the Gen III honey net engineering for improving IDSs to ensure neighborhood generation systems. Then various half-breed honey pots rose[15] since they can gather dataset son both of point by point assault procedures and enormous system space inclusion. Among the semixture honey pot designs, the traffic redirection component is planned to interface the frontends and the backend. It is utilized to channel and divert the intriguing traffic into the HIH for top to bottom examination. The half breed honeypot system [14] essentially utilized the Honey nets work in non-Straight forward intermediary to divert the traffic into HIHs. Because of the way that this

approach does not have a traffic separating component, the back ends can be overwhelmed by invalid information effectively. Likewise, the non-straightforward intermediary approach has the indistinguishable unique mark issue since the frontends and back ends are allotted with various IP addresses. Some other cross breed honeypots utilized GRE burrow to divert the traffic, yet the indistinguishable unique mark issue between the frontends and back ends was as yet unsolved, and all traffic was simply treated by the frontend with two coarse-grained modes: dispose of or forward. Rather, in [12] the TCP association replay approach was applied for encouraging the association movement from LIHs to HIHs. Specifically, the straight forward Honeybrid intermediary/portal was proposed in [12], where the creator utilized the libnetfilter_queue to process parcels, with the goal that security analysts can pickup understanding into the specialized detail. In any case, they didn't address the indistinguishable unique mark issue. Afterward, a few arrangements were displayed to address the indistinguishable unique mark issue dependent on the straightforward Honeybrid passage. Lengyel et al. proposed a half and half honey nets design in particular VMI-Honeymon.

Programming characterized organizing (SDN) expects to isolate the framework that decides the bearing of traffic (control plane) from the hidden frameworks that forward traffic to the chose goal (information plane). Thus, the capacity of stream control is the intrinsic bit of leeway of SDN. The programmable SDN-based system can enable the framework director to progressively arrange the information plane as per the prerequisites. The SDN innovation are as of now broadly utilized in the field of system security of conveyed frameworks. As of late, a few SDN-empowered honey pot frameworks have been proposed. Hog Mapis a synergistic honey pot framework basically. It receives SDN innovation to disentangle commercial center coordination crosswise over various are as to take an interest in Hog Map, different suppliers with assorted system designs just should be furnished with an Open Flow switch and the Hog Map-guaranteed SDN applications, which empower the supplier to take an interest indifferent administrations and perform in the nick of time activities to advance traffic without manual setup. Hog Map utilizes a parcel replay based session movement instrument. Be that as it may, it didn't portray how to give stealth, for example the most effective method to take care of the in distinguishable unique finger impression issue. Honey Mix is another in triguing SDN-based shrewd honey net, which used to at the same time set up various associations with a lot of honeypots and select the most alluring association with motivate assailants to stay associated. The disarray is whether the honey pots containing similar administrations utilize the in distinguishable unique mark. Except if the framework tended to this issue, or else it might neglect to pipe the association between the honeypot and the change to the one between the switch what's more, the assailant. Honey Proxy [13]proposed the fundamental segment utilized in Honey Mix. The intermediary module circulates the solicitations what's more, chooses the most fitting reaction for the assailant to collaborate with. So as to convey vindictive traffic to pertinent honeypots and select the most proper answer from various reactions of the honeypots, the creators planned three modes: Straightforward Mode (T-Mode) to advance the filtering or login endeavors to an IDS prepared LIH; Multicast Mode (M-Mode) to conveyance the payload bundle to all related honeypots also, decide the best answer reacting the aggressor all together to balance fingerprinting assaults; Relay Mode(R-Mode)to keep up an elite association between the aggressor also, the HIH. This methodology can adequately deal with the association and give proper answer. Be that as it may, on the grounds that Honey Proxy speaks to the entire honey net as a black box that runs numerous helpless administrations, the significant downside is that the Honey Proxyisa non-straightforward intermediary stowing away all its internal individual little honeypots other than uncovered them straight forwardly. One framework including numerous helpless administrations most likely will cause the enemy's suspension, in this manner it defies the standard of wide information catch and stealthy information control. A keen honeynet design dependent on the SDS structure is proposed, empowering adaptable arrangement what's more, dynamic provisioning over Network Function Virtualization Foundation (NFVI). This paper centers on moving assets as indicated by the remaining burdens of every honeypot and control off unused modules, which is a sort of counter measure that expands the cost-effectiveness of the honeypot asset. Be that as it may, that isn't the basic issue in honeypot examine setting. The plan of the traffic sending part is indistinct: on the off chance that it is non-straightforward, at that point it has the comparable issue with Honey Proxy when powerfully dispatching the traffic; if it is straightforward, at that point it comes up short on the method forgiving stealthy traffic and asset relocation.

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 3 March 2020

3. HONEYDOC ARCHITECTURE



The Honey DOC decouples the Captor and the Decoy from the engineering perspective, and by utilizing the Orchestrator to facilitate them, it can effectively empower all-round honey pot plan. We previously saw that the distinction between a honeypot and a helpless framework is that a honeypot must be trusted yet a helpless framework is untrusted. In this way, honeypot must have some security program to make it trusted. Fan [16] indicated that the security level ought to be upgraded alongside the association level in setting of honeypot. The paper isolated the captor from the fake, and the captor really speaks to the security program in setting of honeypot. Be that as it may, during the previous long stretches of honey pot advancement, the captor has not gotten enough consideration, and there commendations were frequently fat bait ands lender captor arrangements, what's more, much of the time, they were not decoupled and the significance of the captor is frequently disregarded (see case 1of the illustration in the Introduction segment). Be that as it may, the truth of the matter is that the captor is assuming an undeniably significant job in (high-caliber) information catch. Already, there was no honeypot design proposition embracing the captor to have a companion status with the imitation, which definitely brought about the frail or constrained captor usefulness in the honeypot. Along these lines, the decoupled Decoy and Captor can release the intensity of the captor for serving the excellent information catch, in the interim, the decoupling carries advantages to the Decoy as all things considered, since it tends to be increasingly adaptable and assorted once it leaves the requirements of the Captor. Likewise, the decoupling is the premise for deftly consolidating the Decoy and Captor to play out aground-breaking honeypot framework (see case 2 of the analogy in the Introduction segment). Since the Captor and Decoy are decoupled, on one hand, they can be grown individually what's more, their ability can be refreshed freely. On the other hand, they can be joined together in various manners to do all the more dominant functionalities.

Nonetheless ,to encourage the mix isn't a simple assignment, which includes work dispatch, work collaboration, and so forth so then another huge module named Orchestrator is profoundly required for the reason of organizing the two modules to run in general honeypot framework. In this way, we propose a novel honeypot framework engineering (see Fig. 1) that decouples the Decoy and Captor two in dependent modules, where they will have a similarly significant status, what's more, they are facilitated by the Orchestrator module. They stem information catch and control applications work cooperatively to encourage the traffic order and re direction, which are utilized to process and control the system information stream sending to the baits. That is affectability applicable, so will be depicted in more detail in subsection IV-C1. The virtual bait deployer is responsible for arranging, making and overseeing heterogeneous baits for information catch. It ought to be sufficiently adaptable to convey diverse single committed fakes as far as the communication levels, and furthermore ought to be capable to deal with a total honeynet including different distractions. Moreover, the frame work information catch application is dependable for getting the frame work action in the HIHs. Likewise, the digital danger data (CTI) information investigation application is pointed to examine the logged CTI information so as to uncover further digital dangers, whereby proper response can be done ahead of time. These counter measure related segments will be portrayed in more detail in subsection IV-C2. Fundamentally, every one of the parts should work in stealth against enemy's doubt. In this paper, we basically center on the stealthy TCP association relocation for diverting the assault stream, which will be depicted in subsection IV-C3.

Multiple grouping criteria

The Network Data Catch Application works with the DE to give an adaptable traffic grouping approach, which permits the client to set subjective guidelines and partner activities (for example Drop, Forward, or Redirect).

There are a few different ways to make traffic arrangement: signature-based (for example payload-based) and source destination based (for example addresses-based). Because of the way that the answer to which traffic merits being examined is emotional what's more, relies upon the security specialist's aim, the framework ought to enable the client to tweak the traffic arrangement. So as to help numerous traffic characterization criteria, we apply a standard based approach to give the adjustable. The methodology for synchronizing Seq and Ack numbers traffic arrangement. The client can set the "activity" field in the rule for handling the coordinated traffic. We think about incorporating

a) NIDS to encourage the Network Data Capture Application to assess the traffic to send the caution message to the DE to settle on relating choice on the traffic.

b) Fine-grained process technique against the characterized information: The RE will do as indicated by the "activity" field of the alarm message. On the off chance that that is "DROP", the RE will dispose of the traffic, finishing the association. In the event that the alarm message demonstrates that the traffic must be sent to either a MIH or an HIH, the RE will keep preparing the stream, choosing the relating SDN switch's out port that connections the objective honeypot and sending the bundle to it. In the interim, the required SDN stream sections will be introduced in the relating SDN to do the TCP succession number synchronization. Therefore, when the TCP association has been moved to the objective honeypot, the NIDS doesn't have to investigate the consequent parcels of that association any more.

Countermeasure

Countermeasure gives the reaction against the assault conduct to improve the productivity of information catch. In a few countermeasures against interruption were exhibited. In like manner, with respect to the honeynet situation, the countermeasures can be partitioned in to three classes: assault stream control, distraction dynamic arrangement, information investigation and defenselessness fix.

a) Attack stream control: This kind of counter measure is the fundamental one with respect to the Data Control portrayed in subsection III-B2. The traffic can be blocked, disposed of, diverted or segregated, upon SDN strategy, all these stream controls can be encouraged by the Network Data Control Application previously mentioned.

b) Decoy dynamic arrangement: Decoy dynamic organization is with respect to the fake auspicious insurgency. Evidently, it is a dull undertaking to arrange and send a honey net physically. The virtual distraction deployer is intended to progressively convey and deal with the honeynet. It underpins some solid counter measures. For example, powerfully convey a distraction to get the moved fascinating traffic; imitate the non-honey pot framework to contain the back-disperse/ outbound traffic; reconfigure the fake's finger prints and the honey net topology to lessen the plausibility of being identified.

c) Vulnerability fix: Vulnerability fix rides on the CTI information investigation, and they frequently bring about a joint countermeasure. CTI information investigation is the solid reflection to the Data Investigation (subsection III-B3).

4. CONCLUSION

A honey pot framework is a crucially significant security office made to be tested, assaulted and bargained, so as to trap the enemies just as research the outstanding, and particularly, the obscure assaults. The development of this paper is the minimized honey pot design-Honey DOC, which varies from the conventional honeypot structures by utilizing the novel Decoy-Orchestrator-Captor point of view to dismember and decouple the honeypot, empowering all-round honeypot plan, which has been shown by the ground-breaking SDN-empowered design. By exploiting the SDN innovation, the heterogeneous distractions upheld by the SDN switches can be incorporated into the adaptable honeypot framework deftly, the various security applications can be created and coordinated upon the SDN controller's APIs, especially, and traffic control can be adaptively and straightforwardly directed by the SDN controller applications as indicated by the prerequisites. A Proof-of-idea framework as been executed for approving the proposition.

The Reasonableness test shows the subjective traffic order rules and the fine-grained activities. The counter measure and stealth tests exhibit that a much steal thier traffic movement work is included however the presentation doesn't diminish contrasted with existing arrangements (for example Honeybrid). Additionally, we led the framework sending virtual honey pots in genuine generation organize for catching live assaults. The genuine information based approval shows the proficiency of information decrease and the adequacy of the traffic redirection for information investigation. The test results show the plausibility what’s more,

effectiveness of the proposed engineering. Later on, we will improve the entire framework and use it to lead explore by long haul live information catch. We consider proposing system capacities virtualization (NFV) based general honeypot deployer, to make and deal with the distractions in cloud, to catch and break down digital risk information from various sources. We additionally find a way to improve the anomaly based recognition, encourage the versatile imitation organization to stop the progressed constant risk (APT), and maybe, collaborate with AI methods to support legal sciences and interruption expectation.

REFERENCES

[1] R.Richardson, "CSI survey2007: The 12th annual computer crimeand security survey," Comput. Secur. Inst., San Francisco, CA, USA, Tech. Rep., 2007.

[2] Internet Security Threat Report, Symantec, Mountain View, CA, USA, 2018.

[3] S. W. Brenner, "Cyberterrorism: How real is the threat?" Media Asia, vol. 29, no. 3, pp. 149–154, 2002.

[4] L. Janczewski, Cyber Warfare and Cyber Terrorism. Hershey, PA, USA: IGI Global, 2007.

[5] L. Spitzner, "HoneyPots: Catching the insider threat," in Proc.19th Annu. Comput. Secur. Appl. Conf., Dec. 2003, pp. 170–179.

[6] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," Comput. Secur., vol. 24, no. 1, pp. 31–43, 2005.

[7] R. P. van Heerden, B. Irwin, and I. Burke, "Classifying network attack scenarios using an ontology," inProc. 7th Int. Conf. Inf. Warfare Secur., 2012, pp. 324–331.

[8] R. McGrew and R. B. Vaughn, Jr., "Experiences with honeypot systems: Development, deployment, and analysis," in Proc.39th Annu. Hawaii Int. Conf. Syst. Sci. (HICSS), vol. 9, Jan. 2006, p.220a.

[9] D.O'Brien, "ISTR ransomware 2017," Symantec, Mountain View, CA, USA, White Paper, 2017.

[10] M. Nawrocki, M. Wählisch, C. Schmidt, T. C. and Keil, and J. Schönfelder. (Aug. 2016). "A survey on honey pot software and data analysis." Available: https://arxiv.org/abs/1608.06249

[11] (May 2006). Know Your Enemy: Honey Nets. Available: http://old.honeynet.org/papers/honey net/

[12] R. Berthier and M. Cukier, "Honeybrid: A hybrid honeypot architecture," in Proc. USENIXSecur. Symp., 2008.

[13] S. Kyung et al., "Honey Proxy: Design and implementation of next generation honeynet via SDN," in Proc. IEEE Conf. Commun. Netw. Secur. (CNS), Oct. 2017, pp. 1–9.

[14] H. Artail, H. Safa, M. Sraj, I. Kuwatly, and Z. Al-Masri, "A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks," Comput. Secur., vol. 25, no. 4, pp. 274–288, Jun. 2006.

[15] G. Portokalidis and H. Bos,"SweetBait:Zero-hour worm detection and containment using low-and high-interaction honeypots," Comput. Netw., vol.51, no. 5, pp. 1256–1274, 2007.

[16] T. K. Lengyel, J. Neumann, S. Maresca, B. D. Payne, and A.Kiayias, "Virtual machine introspection in a hybrid honeypot architecture," presented the5thWorkshop Cyber Secur. Exp. Test, Berkeley, CA, USA, 2012.

[17] H.Wang and Q.Chen, "Dynamic deploying distributed low-interaction honey net," J.Comput., vol. 7, no. 3, pp. 692–698,2012.

