www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-2, April 2018
Review Paper

Int. J. Sc. Res. in
Network Security
and Communication

ISSN: 2321-3256

Honeypots: Virtual Network Intrusion Monitoring System

Manmohan Dagar[1*], Rashmi Popli[2]

[1*]Department of Computer Networking, YMCA University of Science and Technology, Faridabad, India
[2] Department of Computer Networking &Information Technology, YMCA University of Science and Technology, Faridabad, India

[*]*Corresponding Author: monty.dagar92@gmail.com, Tel.: +91-9999334327*

Received: 06/April/2018, Revised: 14/April/2018, Accepted: 22/April/2018, Published: 30/Apr/2018

***Abstract*—** In the past several years there has been extensive research into honeypot technologies, primarily for detection and information gathering against external threats. However, little research has been done for one of the most dangerous threats, the advance insider and the trusted individual who knows your internal organization. These individuals are not after your systems, they are after your information. This paper discusses how honeypot technologies can be used to detect, identify, and gather information on these specific threats.

Keywords— Honeypot, Intrusion Detection System (IDS), Honeyd, Load Balancer, Honeycomb and Honeywall.

I. INTRODUCTION

Honeypots are security resources whose value is being attacked, comprised or probed.” The honeypots are security resource. This security resources may come in different shapes and sizes. In fact, Honeypot could just as simply be one of your old PC’s, a script or even a digital entity like some made-up patient records. Whose value is being attacked, comprised or probed. If anyone “touches” our Honeypot, then we know someone’s creeping around in our network system, no person or resource should be communicating with it. Incoming traffic or more dangerously, outgoing traffic would be considered unauthorized traffic. A Honeypot is a security resource whose value is in its being probed, attacked or compromised. A Honeypot could come in different sizes. It can be one of your old PC’s, a script like Honeyd or even more complicated setups like the Honeynet. [1]

The Honeypots looks and acts like a production systems but in reality is not so. Since its’ not a production system, no one’s supposed to use it thus should have no valid traffic. So if we detect traffic, most likely its potentially malicious traffic.

Definition: “A honeypot is a faked vulnerable system used for the purpose of being attacked, probed, exploited and compromised.”

There are resources that has no authorized activities, they do not have any production value. Theoretically, Honeypot should see no traffic because it has no legal activity.

This means any interaction with a honeypot is most likely unauthorized or malicious activity. Any connection attempts to the honeypots are most likely an attack, compromise or probe. While this concept sounds very simple, it is this very simple that give honeypots their tremendous advantages.

II. TYPES OF HONEYPOT

Honey are classified on the basis of their deployment and based on their level of involvement and based on the deployment, honeypots may be classified as:

- Production Honeypots
- Research Honeypots

A. *Production honeypots*

They are easy to use, capture only limited information, and are used by corporations or companies. Production honeypots are placed inside the production network with other production servers by organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots do. The purpose of a production honeypot is to help mitigate risk in an organization. The honeypot adds value to the security measures of an organization. [10]

B. *Research honeypots*

They are run by a volunteers, non-profit research organization or an educational institution to gather information about the motives and tactics of the BLACKHAT community targeting different networks. These honeypots do not add direct value to a specific organization. Instead they are used to research the threats organizations

© 2018, IJSRNSC All Rights Reserved

face, and to learn how to better protect against those threats. This information is then used to protect against those threats. Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations. [2]

Honeypots are targeted in the network by the hackers, and depending on the setup provided, it can be difficult to detect but sometimes not. If it is a high-interaction honeypot, it will run everything as the real system works, and thus, can be very difficult to detect. Whereas a low-interaction honeypot can be easily detected once the attacker is inside. It will have fewer processes running, and many basic tools are missing which leads the network to expose. Some of the intruders may fail to save files over different sessions, and some may obstruct all outgoing connections. Essentially it depends entirely on how the honeypot was set up. Thus, there is not any particular method of detecting honeypots. If a precise method to detect honeypots is discovered, new honeypots will instantly come into play to neutralize the method.

III. LITERATURE REVIEW

A. Before you Michael Bailey, Evan Cooke, Farnam Jahanian, Yunjing Xu, and Manish Karir.A Survey of Botnet Technology and Defenses. [October 11 2017].

Global Internet threats have undergone a profound transformation from attacks designed solely to disable infrastructure to those that also target people and organizations. At the center of many of these attacks are collections of compromised computers, or Botnets, remotely controlled by the attackers, and whose members are located in homes, schools, businesses, and governments around the world. In this survey paper we understood how existing botnet works, the evolution and future of botnets, as well as the goals and visibility of today's networks intersect to inform the field of botnet technology and defense. [4]

B. Abigail Paradise, Asaf Shabtai, Rami Puzis - Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks. [14 July 2017]

Reconnaissance is the initial and essential phase of a successful advanced persistent threat (APT).There are many cases in which attackers collect information from social media, such as educational social networks, professional social networks etc. This information is used to select members that can be exploited to penetrate the organization. Detecting such reconnaissance activity is extremely hard because it is performed outside the organization's premises. [5]

C. Kun Wang, Miao Du, Sabita Maharjan - Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid. [16 February 2017]

Advanced metering infrastructure (AMI) is a component for a smart grid system that is used to measure, collect, store, analyze, and operate user's consumption data. The need of communication and data transmission between consumers (smart meters) and utilities make AMI vulnerable to various attacks. In this paper, we focus on distributed denial of service attack in the AMI network. We introduce honeypots into the AMI network as a decoy system to detect and gather attack information. We analyze the interactions between the attackers and the defenders, and derive optimal strategies for both sides. We further prove the existence of several Bayesian-Nash equilibriums in the honeypot game. Finally, we evaluate our proposals on an AMI testbed in the smart grid, and the results show that our proposed strategy is effective in improving the efficiency of defense with the deployment of honeypots. [12]

D. R. Piggin, I. Buffey - Active defence using an operational technology honeypot. [16 February 2017]

This paper presents research to examine the benefits of deploying a high interaction hardware Operational Technology (OT) or Industrial Control System (ICS) honeypot, as opposed to a virtualized system. The Honeypot Project successfully developed and demonstrated an innovative approach to implementing a situational awareness capability in an operational industrial control system environment. The approach also contributes to an organization's potential forensics capability for ICS systems. Furthermore, this has been achieved via a remote access platform without disrupting operations, whilst preserving vital evidence. The Honeypot project has demonstrated new techniques to enhance monitoring of ICS systems, indicated further benefits and illustrated where such approaches would be suitable. [16]

E. Nikita M. Danchenko, Anton O. Prokofiev, Dmitry S. Silnov - Detecting suspicious activity on remote desktop protocols using Honeypot system. [27 April 2017]

This article defines the effectiveness of security systems using Honeypot technology. There are studied basic structures of security systems, which use Honeypot technology. There is described developing process of a "trap" for VNC/RDP protocols, which main goal is to emulate remote desktops. Assembled "trap" will identify the attacker to collect information about his actions by analyzing malicious traffic (Honeypot resource allows to collect only malicious traffic unlike firewall which gathers all the traffic). [17]

IV. ADVANTAGES OF HONEYPOT

- Small Data sets: Honeypots only monitors attacks, unauthorized activity, dramatically reducing the amount of data they collect. Organizations that may log thousands of alerts in a day may only log a hundred alerts with honeypots. This makes the data honeypots collect much easier to manage and analyze.
- Reduced False Positives: Honeypots reduce false alerts, as they only capture unauthorized activity.

- Catching False Negatives: Honeypots can easily identify and capture new attacks never seen before.
- Minimal Resources: Honeypots require minimal resources, even on the largest of networks. This makes them an extremely cost effective solution.
- Encryption: Honeypots can capture encrypted attacks.

V. APPLICATION AND DEPLOYMENT OF HONEYPOTS

A. Honeypots in Educational Resource

Honeypots in Educational Resource Jeremiah K. Jones & Gordon W. Romney discussed the aspects of using the honeynets in educational areas. A lab has been established at Brigham Young University for network security purpose for undergraduate and graduate students called ITSecLab. They use this lab for tracing the malicious traffic in the network. This lab was designed for the 602 purpose of experiments that works on network security by the students. In addition to this lab they have implemented a honeypot in their lab to get in touch with blackhats and explore its uses as an educational tool. The lab is designed as an isolated “Sandbox” in order to keep away the malicious activities from lab. The honeypot is implemented at Brigham Young University keeping in mind the certain benefits such as it notifies about the new threats, securing the lab at higher level, learning the network and security basics and closely identifies the flaws. One more aspect comes into play when implementing the honeypot, the legal issues that are most important part in implementation because if the honeypot gets compromised and is used as zombie then the owner has to suffer the loss. [3][18]

*B. **Honeypot with IDS***

An Intrusion Detection System (IDS) discriminates between the traffic coming from various clients and from the attackers, in an effort to simultaneously ease the problems of throughput, latency and security of the network. After that we can present the results of a sequence of load and their response time in the terms of performance and scalability tests, and suggest various types of potential uses for such a system. In IDS we may use two common type detection level known as Misuse detection and Anomaly detection. In misuse detection the IDS analyzes all the various kinds of information that have collected and match it to large database of attack signatures. In anomaly detection the administrator makes a baseline, or we may say a normal network traffic load, collapse, protocol and packet size. It monitors network and compares it to those baseline. IDS can be further categorizes into Network based and Host based. In network based IDS, the individual packets are analyzed whereas in host based IDS all the activities of the host are monitored. Honeypots can either be host and/or network based, but generally they are not network based as all interface operations are typically performed over a network connection. Its key utility is that it simplifies the Intrusion Detection problem of separating “anomalous” from “normal”. Thus any activity on a Honeypot can be immediately defined as abnormal. From the below diagram each components play a specific role in implementation of honeypot with IDS within a network. Initially load balancer receives the virtual IP address, and checks whether the packet containing the request has been fragmented, and then it is reassembled. Then load balancer opens a TCP connection to the IDS Process, and sends the content of the packet (less the headers) over that connection. IDS checks the content of packets against its database and returns the Boolean value of that to load balancer through the same TCP connection. After receiving the result, the load balancer closes the TCP connection. If the result from the IDS was “true” (Indicating an attack) the packet is forwarded to the Honeypot. Otherwise, a server is selected from the active server pool in a round-robin fashion and the packet is forwarded to the server.

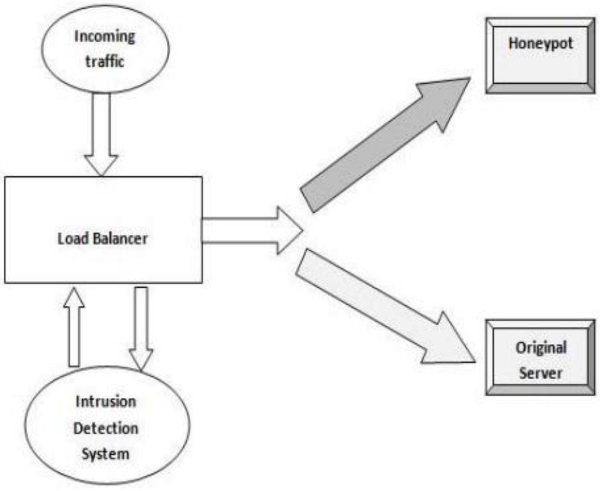

Figure 1: Flow of packets Through IDS in Honeypot

*C. **Network Security through “Hybrid Honeypot”***

Here honeypots is divided into two categories according to their level of interaction, low level interaction and high level interaction. The level of interaction can be defined as the maximum range of attack possibilities that a honeypot allows an intruder to have. In high-level interaction honeypot, attacker interact with real operating systems, all the services and programs and this type of interaction can be used to observe the attackers performance, their tools, motivation and explored vulnerabilities. This type of high-level interaction honeypot can be deploying inside a virtual machine using various virtualization software such as VMware, Qemu and Xen. Example of high-level interaction honeypot is honeynet. It is a network of multiple systems. Honeynet can collect deep information about intruders, such as their keystrokes when they compromise with a system, their chatting sessions with fellow blackhats, or the various tools they use to explore and develop susceptible systems. On low-level interaction honeypot, there is no operating system that an intruder can operate on. All the tools are installed in order to emulate OS and other services.[19] And they all work together with the intruders and infected code. This will reduce the risk radically. This type of honeypot has a few chance of being compromised. These are production honeypots. Typical use of low-level interaction honeypot includes; port scans identification, generation of attack signatures, trend analysis and malware collection. [7]

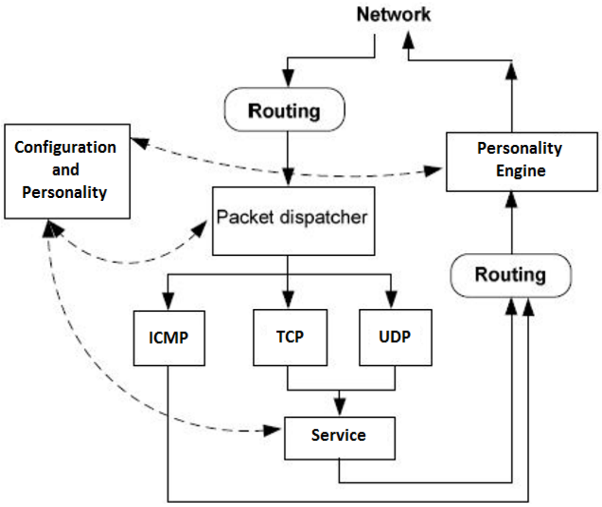

Figure 2: Simplified view of Honeyd Architecture

In the above figure we deploy Hybrid Honeypot by using both Low-level and high-level interaction honeypot. To offer an extensible infrastructure for honeypot installation and growth of detection mechanisms on top, good features of both types have to be combined. Here in this type of system, low-level interaction honeypot act as lightweight proxy. As we require high-level interaction honeypot to process all traffic destined to block IP address space. [11]

*D. **Deployment of Intrusion Detection Signatures using Honeycomb***

This deployment deals with generation of signatures. At present generating signatures are tiresome work, manual process that needs detailed knowledge of each software function that is supposed to be detained. Simple signatures tend to generate large numbers of false positives, too specific ones cause false negatives. For the same reason the concept of Honeycomb a system that generates signature for infected traffic automatically, is used. Here pattern-detection techniques and packet header are used for conformance tests on traffic captured by honeypots [14]. The purpose discussed about the attack signatures is to explain the characteristic elements of attacks. Right now we don't have any such standard for defining these signatures. As a consequence, different systems offer signature languages of varying expressiveness. A good signature must be narrow enough to confine precisely the characteristic aspects of exploit it attempts to address; at the same time, it should be flexible enough to capture variations of the attack. Failure in one way or the other leads to either large amounts of false positives or false negatives. [15]

VI. DISADVANTAGES OF HONEYPOTS

- Single Data Point: Honeypots all share one huge drawback; they are worthless if no one attacks them. Yes, they can accomplish wonderful things, but if the attacker does not sent any packets to the honeypot, the honeypot will be unaware of any unauthorized activity.
- Risk: Honeypots introduces risk to our environment. As different honeypots have different levels of risk. Some introduce very little risk, while others give the attacker entire platforms from which to launch new attacks, Risk is variable, depending on how one builds and deploys the honeypot.

VII. CONCLUSION

Honeypot is just a tool. How we use that tool is up to us. There are a variety of honeypot options, each having different value to organizations. We have categorized two types of honeypots, production and research.

As our dependence on computers and network constantly increases, comprehensive network security is of tremendous importance. First requirement to be able to better protect networks assets is to gain a detailed understanding of malicious threats. There are innumerable options available today to access any sensitive information maliciously. Therefore, to counter such attacks the concept of honeypot has been precisely invented to fill this task. This system gave us an opportunity to study honeypot and ids system in detail. It is important for organizations to secure their digital assets by detecting and preventing vulnerabilities before they are exploited. Production honeypots help reduce risk in an organization. Research honeypots are different in that they are not used to protect a specific organization. Instead they are used as a research tool to study and identify the threats in the Internet community. Regardless of what type of honeypot you use, keep in mind the 'level of interaction'. This means that the more your honeypot can do and the more you can learn from it, the more risk that potentially exists. Honeypots will not solve an organization's security problems. Only best practices can do that. However, honeypots may be a tool to help contribute to those best practices.

.

REFERENCES

[1] Spitzner, L. 2002. Honeypots: Tracking Hackers. 1st ed. Boston, MA, USA: Addison Wesley.

[2] Mokube, I. & Adams M., 2007. Honeypots: Concepts, Approaches, and Challenges. ACMSE 2007, March 23-24, 2007, Winston-Salem, North Carolina, USA.

[3] Aaron Lanoy and Gordon W. Romney, Senior Member. A Virtual Honey Net as a Teaching Resource," 2006 7th International Conference on Information Technology Based Higher Education and Training, Ultimo, NSW, pp. 666-669, 2006.

[4] A Survey of Botnet Technology and Defenses. Available from: M. Bailey, E. Cooke, F. Jahanian, Y. Xu and M. Karir, "A Survey of Botnet Technology and Defenses," 2009 Cybersecurity Applications & Technology Conference for Homeland Security, Washington, DC, pp. 299-304, 2009.

[5] Abigail Paradise, Asaf Shabtai, Rami Puzis - "Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks," in IEEE Transactions on Computational Social Systems, vol. 4, no. 3, pp. 65-79, Sept. 2017.

[6] S. Kemp. Digital in 2017: Global Overview, accessed on Jan. 24, 2017.

[7] The Honeynet Project. (2014). "Outsmarting the smart meter"

[8] Kun Wang, Miao Du, Sabita Maharjan - "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid," in *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2474-2482, Sept. 2017.

[9] J. Markert and M. Massoth, "Honeypot framework for wireless sensor networks," in Proc. Int. Conf. Adv. Mob. Comput. Mult., Dec. 2013.

[10] V. Pothamsetty and M. Franz, SCADA HoneyNet Project: Building Honeypots for Industrial Networks, tech. report, Cisco Systems, 2005

[11] N. Provos, Developments of the Honeyd Virtual Honeypot, user forum, 2008

[12] Kun Wang, Miao Du, Sabita Maharjan - "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid," in *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2474-2482, Sept. 2017.

[13] The Honeynet Project, Honeywall, 2016.

[14] V. Paxson, .Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks (Amsterdam, Netherlands: 1999), vol. 31, no. 23-24, pp. 2435.2463, 1998.

[15] M. Roesch, .Snort: Lightweight Intrusion Detection for Networks. In Proceedings of the 13th Conference on Systems Administration, 1999

[16] R. Piggin, I. Buffey - "Active defence using an operational technology honeypot," *11th International Conference on System Safety and Cyber-Security (SSCS 2016)*, London, pp. 1-6, 2016.

[17] Nikita M. Danchenko, Anton O. Prokofiev, Dmitry S. Silnov "Detecting suspicious activity on remote desktop protocols using Honeypot system," *2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, St. Petersburg, pp. 127-128, 2017.

[18] Pradeep Chouksey, "*Study of Routing in Ad hoc network*", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.2, pp.55-57, 2017.

[19] M. Arora, S. Sharma, "*Synthesis of Cryptography and Security Attacks*", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.5, pp.1-5, 2017

Authors Profile

Manmohan Dagar pursed Bachelor of Technology from Manav Rachna International University, India in 2015 and currently pursuing Master of Technology in the field of Computer Networks from YMCA University of Science & Technology Faridabad, India. He is currently working on Network Security, Cyber Security, Cryptographic Mechanisms and Software Engineering.

Dr. Rashmi Popli pursued Bachelor of Engineering from Career Institute of Science and Technology Faridabad, India, Master of Science from CITM and pursued Ph.D. from YMCA University currently working as Assistant Professor in Department of Computer Engineering in YMCA University Faridabad, India since 2005. She has published more than 27 research papers in reputed international journals and it's also available online. She has 14 years of Teaching and Research Experience.