International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 07th Jun 2022.
Link: https://ijiemr.org/downloads/Volume-11/Issue-06

DOI: 10.48047/IJIEMR/V11/I06/75

Title: **A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks**

Volume 11, Issue 06, Pages 1413-1418
Paper Authors: **Salimova Husniya Rustamovna1*, Bobomurodov Sharofiddin Azimjon o'g'li2*, Ganiyev Asadullo Mahmud o'g'li3***

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks

Salimova Husniya Rustamovna1*, Bobomurodov Sharofiddin Azimjon o'g'li2*, Ganiyev Asadullo Mahmud o'g'li3*

1*Master's degree, Faculty of Cyber-Security, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

2* Bachelor degree, Faculty of Radio and Mobile Communications, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

3* Bachelor degree, Faculty of Software engineering, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

ABSTRACT: Attacks on the internet keep on increasing and it causes harm to our security system. In order to minimize this threat, it is necessary to have a security system that has the ability to detect zero-day attacks and block them. "Honeypot is the proactive defense technology, in which resources placed in a network with the aim to observe and capture new attacks". This paper proposes a honeypot-based model for intrusion detection system (IDS) to obtain the best useful data about the attacker. The ability and the limitations of Honeypots were tested and aspects of it that need to be improved were identified. In the future, we aim to use this trend for early prevention so that pre-emptive action is taken before any unexpected harm to our security system.

Keywords: Honeypot, network, detection system, hybrid, protect, framework, hacker

INTRODUCTION

The Internet is a network of networks. It is based on the concept of packet switching. Though the services offered by Internet are extensively used from a layman to multi-millionaire it also has its own defects. Many attacks on Internet are being identified and reported. Some of the common types of network attacks are saves dropping, data modification, identity spoofing, password-based attacks and denial of service attacks. To overcome all these types of attacks an organisation usually installs an intrusion detection system to protect the confidential data exchanged over its network. The local network is then connected to the Internet thereby availing the employees to be online on the fly. Information security has three main objectives namely 1. Data confidentiality 2.Data integrity 3. Data availability. Data confidentiality ensures that the secure data can be accessed only by authorized persons. Data integrity allows secure modification of data. Data availability ensures that the data is available readily to authorized persons. Small scale industries often do not prefer on intrusion detection systems due to its installation and maintenance costs.

Materials: Honeypots are mostly used by military, research and government organizations. They are capturing a huge amount of information. Their aim is to discover new threats and learn more about the Blackhat motives and techniques. The objective is to learn how to

protect a system better, they do not bring any direct value to the security of an organization.

Methods: They are simple as they do not require high end algorithms, configurations. Also they are much easy to use. Simply deploy them and monitor is what we require to do. Honeypots are quite valuable as it quickly captures the malicious activities. It reflects the security mechanism level of the system. Various security mechanisms provide a potential amount of false positive alert messages but honeypots do not provide false positives as it is mostly accessed by the intruders. Also, additionally honeypots help to understand various new vulnerabilities, threats and attack patterns.

Results: We studied all level of interaction honeypots and configured them. The evolution of honeypots can also be understood by looking at the ways these systems are being used in association with IDSs to prevent, detect and help respond to attacks. Indeed, honeypots are increasingly finding their place alongside network- and host-based intrusion-protection systems. Honeypots are able to prevent attacks in several ways. The first is by slowing down or stopping automated attacks, such as worms or autorooters. These are attacks that randomly scan an entire network looking for vulnerable systems. (Honeypots use a variety of TCP tricks to put an attacker in a "holding pattern.") The second way is by deterring human attacks. Here honeypots aim to sidetrack an attacker, making him devote attention to activities that cause neither harm nor loss while giving an organization time to respond and block the attack. As noted above, honeypots can provide early detection of attacks by addressing many of the problems associated with traditional IDSs, such as false positives and the inability to detect new types of attacks, or zero-day attacks. But increasingly, honeypots are also being used to detect insider attacks, which are usually more subtle and more costly than external attacks. Honeypots are also helping organizations respond to attacks. A hacked production system can be difficult to analyze, since it's hard to determine what's normal day-to-day activity and what's intruder activity. Honeypots, by capturing only unauthorized activity, can be effective as an incident-response tool because they can be taken off-line for analysis without affecting business operations. The newest honeypots boast stronger threat-response mechanisms, including the ability to shut down systems based on attacker activity and frequency-based policies that enable security administrators to control the actions of an attacker in the honeypot.

Conclusion: We explained honeypot systems in detail, and implemented low interaction, middle interaction and high interaction honeypots at laboratory. Our goal was to understand their strategy and how they are working in order to lure intruders towards the system. We discovered their security flaws in order to help researchers and organizations. Several companies are using honeypot systems to protect the whole organization's network security, and researchers are making academic experiments on them at schools. As we all know network security is very significant for all computer systems because any unprotected machine in a network can be compromised in any minute. One may lose all the secret and important data of a company, which can be a great loss, and it is also very dangerous that someone else knows your important personal information. Thus, we tried to find answers for honeypots' security using all interaction honeypots possible. Our main goal for our thesis was to see if honeypots are easy to hack and check if they are really isolated from other networks like a organization's network. When a honeypot is

compromised, is it possible to reach other systems and compromise them too ? After the system is compromised, is it possible to track the hacker by using necessary forensic science tools ? How efficient are they ? As we stated in results and analysis part,we easily hacked all the honeypots that we used for our thesis. Especially, low interaction honeypot Honeyd can be hacked easily without too much effort. As we stated before, any amateur hacker can seize the system and also can see that it is a trap system. Therefore, Honeyd is not a good honeypot as its features are not efficient to fool the hacker. As Honeyd is a deamon, it is just simulating a operating system's services. So, it is not possible to a hacker to seize other systems using Honeyd. For the intruder, it will not take time to see that the system is not real, so he will not continue compromising it. He will leave the system. For forensic part, Honeyd's log was sufficient to see the actions of the hacker. Next part was to try Nepenthes as medium interaction honeypots. The result was quite similar. Thus,we came up with this conclusion: Low interaction honeypots and medium interaction honeypots are just simulating the services of a real system, because of that it is not possible to capture significant data from intruders. They are slightly different from each other but the main idea is the same. As they are not real operating systems , it is not risky to build them. There is no need to mention about further attacks. So, we moved on to the last level. After working low interaction and medium interaction honeypots, we decided to deploy high interaction honeypots. We studied on Honeywall. Even though it is time consuming and difficult, we managed to create a structure and worked on it. Our result were more interesting than before.High interaction honeypots are not virtualizing the system. They are real systems.So, it is very risky but the captured information is important. After deploying the implementation correctly, we successfully hacked the honeynet, but not Honeywall itself. It was the result we were looking for. As we stated in this paper, honeypot systems are still very new but are a great tool to identify cyber threats. The problem nowadays is that a very good hacker will most likely be able to understand when he is attacking a honeypot. Low interaction honeypots will be able to identify mostly automated attack and will hardly be able to understand new hacker method. On the other hand, high interaction systems are here to entrap the hacker and make him give away his techniques and tools to the forensic team. The network administrator implementing this kind of honeypot should make sure that the system is completely isolated 33 from the production network. This is the best defense if the hacker compromises the honeypot. Network security is not a path many students are taking but we see it as one of the most important topics when we speak about computing. We were curious about this subject and decided to write a thesis on that field. This work taught us a lot about the black hat and white hat community. It also gave us an idea how huge and complex the forensic work is. New threats are discovered everyday and the best way to stay protected is to always stay up to date. By doing this simple task, most attacks will not have any effect on the system. The problem nowadays is that people using pirated version of an operating system are contributing to botnets. Their system does not support critical updates and they are more sensitive to automated attacks. Nowadays, the implementation and development of honeypots are under control by network security expert. The weakness of this system is that it is not backed up by a clear legislation. Most of the work in the future should be about improving the laws about honeypots. The current laws about honeypots in

most of the countries are not clear. There is a gap between the lawyers and the IT professionals. They should learn to cooperate with each other in order to clarify the legislation and give a clear answer about the legality of this technology. A lot of work should be done in the future to improve this situation. On a technical aspect, the main difficulty is to keep up with the new attacks. These days, it is not hard to detect a honeypot system, most of the work should focus on making this technology stealthier.

References:

1. Y. Yun, Y. Hongli and M. Jia, "Design of distributed honeypot system based on intrusion tracking", 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), pp. 196-198, 2011.
2. J.C. Chang and T. Vi-Lang, "Design of virtual honeynet collaboration system in existing security research networks", 2010 International Symposium on Communications and Information Technologies (ISCIT), pp. 798-803, 2010.
3. L. Li, H. Sun and Z. Zhang, The Research and Design of Honeypot System Applied in the LAN Security in Beijing, pp. 360-363, 2011.
4. L. J. Zhang, "Honeypot-based defense system research and design", Computer Science and Information Technology 2009. ICCSIT 2009. 2nd IEEE International Conference on, pp. 466-470, 2009.
5. T. Holz and F. Raynal, "Detecting honeypots and other suspicious environments", Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop 2005. IAW '05., pp. 29-36, 2005.
6. T. Zhi-Hong, F. Bin-Xing and Y. Xiao-Chun, "An architecture for intrusion detection using honey pot", Machine Learning and Cybernetics 2003 International Conference on, vol. 2094, pp. 2096-2100, 2003.
7. I. Kuwatly, M. Sraj, Z. Al Masri and H. Artail, "A dynamic honeypot design for intrusion detection", Pervasive Services 2004. ICPS 2004. IEEE/ACS International Conference on IEEE, pp. 95-104, 2004.
8. A. Herrero, U. Zurutuza and E. Corchado, "A Neural-Visualization IDS for Honeynet Data", International Journal of Neural Systems, vol. 22, 2012.
9. D. Puthal, S. Nepal, R. Ranjan and J. Chen, "A Dynamic Key Length Based Approach for Real-Time Security Verification of Big Sensing Data Stream" in Web Information Systems Engineering-WISE, Springer International Publishing, pp. 93-108, 2015.
10. Y. Mai, R. Upadrashta, X. Su and J. Honeypot, "A java-based network deception tool with monitoring and intrusion detection" in , Las Vegas, NV, pp. 804-808, 2004.
11. D. Puthal, S. Nepal, R. Ranjan and J. Chen, "DPBSV-An Efficient and Secure Scheme for Big Sensing data Stream", Tustcom/BigDataSE/ISPA2015 IEEE, vol. 1, pp. 246-253.
12. R. Talabis, "Honeypots 101: A Brief History of HoneyPots", The Philippine honeynet project, 2002.
13. R. Baumann, "Honeyd-A low involvement Honeypot in Action", Original published as part of the GCIA practical, vol. 14, 2003.

14. X. Li and D. Liu, "Automatic scheme to construct Snort rules from honeypots data", Journal of Systems Engineering and Electronics, vol. 16, pp. 466-470, 2005.
15. H. Artail, H. Safa, M. Sraj, I. Kuwatly and Z. AI-Masri, "A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks", Computers and Security, vol. 25, pp. 274-288, 2006.
16. D. Dagon, X. Qin, O. Gu, W. Lee, J. Grizzard, J. Levine, et al., Honey stat: Local worm detection using honeypots, pp. 39-58, 2004.