ANALYSIS OF SINGLE HONEYPOT AND USING FIREWALL INTRAINING ATTACK ON WIRELESS NETWORK

Salimova Husniya Rustamovna[1*], Jovliyev Abbosjon Mirmuhsin o'g'li[2*]

[1] Master's degree, specialty "Information Security", Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan*

[2] Bachelor degree, Faculty of "Computer engineering", Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan*

Abstract: Day by day, more and more people are using internet all over the world. It is becoming a part of everyone's life. People are checking their e-mails, surfing over internet, purchasing goods, playing online games, paying bills on the internet etc. However, while performing all these things, how many people know about security? Do they know the risk of being attacked, infecting by malicious software? Even some of the malicious software are spreading over network to create more threats by users. How many users are aware of that their computer may be used as zombie computers to target other victim systems? As technology is growing rapidly, newer attacks are appearing. Security is a key point to get over all these problems. In this thesis, we will make a real life scenario, using honeypots. Honeypot is a well designed system that attracts hackers into it. By luring the hacker into the system, it is possible to monitor the processes that are started and running on the system by hacker. In other words, honeypot is a trap machine which looks like a real system in order to attract the attacker. The aim of the honeypot is analyzing, understanding, watching and tracking hacker's behaviours in order to create more secure systems. Honeypot is great way to improve network security administrators' knowledge and learn how to get information from a victim system using forensic tools. Honeypot is also very useful for future threats to keep track of new technology attacks.

Keywords: Honeypot, low interaction, firewallmikrotik, wireless

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: Honeypot can literally be a computer which can act as a source for attacks. It attracts the hackers to try hacking it which in turn may log the techniques used by the attackers. This log is useful to prevent such attacks to the legitimate network. Honeypot computer usually do not have any important data or information to be secured. It only has fake services running on its ports to attract the attackers.

Methods: Production honeypots are easily deployed in the live environment that may capture only some amount of information about the attacks. Research honeypot deployment is complicated and used mainly for research purposed by government organizations. On the basis of design, honeypots can be divided into 1.Pure honeypots, 2.High-interaction honeypots, and 3.Low-interaction honeypots. Pure honeypots are complete production systems. The honeypot computer is linked to the network and taps the attacks. Low-interaction honeypots allows restricted interaction with attackers and hence they are not infected by the attacks. High-interaction honeypots are vulnerable to attacks. No emulation takes place and hence

more prone to get infected by attacks. Honeynet is a collection of honeypots installed to trap the attacker activities and log them.

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: Honeypots are a potential tool in the world of security. They provide an added benefit if they are used with firewalls or intrusion detection systems. They are available for commercial as well as research purposes and are quite flexible to fulfill our requirements. Honeypots have been used in

various deception techniques like Honey farms, Simple port listener, honeypots as mobile code throttlers, Random Servers, digital breadcrumbs. Thorough care must be taken while deploying honeypots as it involves substantial amount of risk. Hence, a tight risk analysis needs to be done prior to deployment. Also strict rules must be framed for the maintenance purpose. They are cheaper, flexible, provide low false positive rate, can extract encrypted data. Laws and legal issues must be considered for deploying honeypot systems. Honeypots can reap great benefits if they are used in a smart way by using various new technology trends.

Literature:

1. William Stallings "Cryptography and Network Security Principles and Practices" Prentice Hall Publication, pp. 581, 2005.

2. Lance Spitnzer "Honeypots: Tracking Hackers" Addison Wisley Longman Publishing Co.in, 2002.

3. Liu Dongxia, Zhang Yongbo, "An Intrusion Detection System Based on Honeypot Technology" , In the Proceedings of 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE2012), Hangzhou, pp. 451-454.

4. Tao, Jing. Immune-based intrusion prevention model [J]. Network and Information, 200907

5. Peng Hong, Wang Cong, Guan Xin "Intrusion Prevention System in the Network of Digital Mine" 2nd International Conference on Computer Engineering and Technology, Volume 6, pp. 296-299, 2010.

6. M. Sqalli, R. AlShaikh, E. Ahmed "Towards Simulating a Virtual Distributed Honeynet at KFUPM: A Case Study" UKSim Fourth European Modeling Symposium on Computer Modelling and Simulation.pp. 316-321, 2010

7. Ariel Bar, Bracha Shapira, Lior Rokach and Moshe Unger, "Identifying Attack Propagation Patterns in Honeypots using Markov Chains Modeling and Complex Networks Analysis" IEEE International Conference on Software Science, Technology and
Engineering , pp. 28-36, 2016.

8. Thesis on "Honeypots in Network Security" by Deniz Akkaya-Fabien Thalgott, School of Computer Science, Physics and Mathematics, Linnaeus University, 29th June 2010.

9. Gérard Wagener. "Self-Adaptive Honeypots Coercing and Assessing Attacker Behaviour" Computer Science [cs]. Institut National Polytechnique de Lorraine - INPL, 2011. English.

10. Jules Pagna Disso, Kevin Jones, Steven Bailey, "A Plausible Solution SCADA Security: Honeypot Systems" Eighth International Conference on Broadband, Wireless Computing, Communication and Applications,pp. 443-448, 2013.

11. Mohammed H. Sqalli, Shoieb Arshad, Mohammad Khalaf, Khaled Salah, "Identifying Scanning Activities in Honeynet Data using Data Mining" Third International Conference on Computational Intelligence, Communication Systems and Networks, pp. 178-183,
2011.

12. A. Mairh, et al., Honeypot in network security: a survey, In: Proceedings of the 2011 International Conference on Communication, Computing & Security. ACM, 2011. p. 600-605.

13. L. Spitzner, Honeypots: Catching the insider threat, In: Computer Security Applications Conference 2003, Proceedings. 19th Annual. IEEE, 2003. p. 170-179, 2003

14. Dissertation on "Deception Techniques Using Honeypots" by Amit D. Lakhani, Information Security Group Royal Holloway, University of London, UK.

15. Keith Harrison, James R. Rutherford, and Gregory B. White "The Honey Community: Use of Combined Organizational Data for Community Protection" 48th Hawaii International Conference on System Sciences, pp. 2288-2297, 2015.