IN THE FIELD OF CYBER-SECURITY AN INTRUSION DETECTION SYSTEM BASED ON HONEYPOT TECHNOLOGY

Salimova Husniya Rustamovna[1*], Bobomurodov Sharofiddin Azimjon o'g'li[2*,]
[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

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, Handheld computers, Decision support systemshacking, security, forensic analysis of honeypots, network.

Introduction: Honeypot systems are extensively used in Intrusion Detection technology. Honeypots can be defined as systems used to entice attackers, intruders, malicious users away from the main systems. Honeypots have been designed with the aim to distract the attackers from critical systems and to gain vital information about their malicious activity. First of all, a honeypot is a computer system. There are files, directories in it just like a real computer. However, the aim of the computer is to attract hackers to fall into it to watch and follow their behavior. So we can define it as a fake system which looks like a real system. They are different than other security systems since they are not only finding one solution to a particular problem, but also they are eligible to apply variety of security problems and finding several approaches for them. For example, they can be used to log malicious activities in a compromised system, they can be also used to learn new threats for users and creating ideas how to get rid of those problems. Honeypot systems are developed with fake information so that it appears important. The system is often equipped with monitors and event loggers. This equipment monitor, keep an eye on all the accesses and activity carried on honeypot. In this way, who so ever accesses honeypot becomes a suspect. Honeypot can be said to be a trap, as it is

set for trapping the adversary. All the data from honeypot is recorded. These records are analyzed to learn about new attack patterns which pose a threat to vital resources. The value of honeypots and the problems they help solve depend on how you build, deploy, and use them. Honeypots are of no use if they are not attacked. Fig. 1 gives an idea of honeypot systems.

Characteristics of Honeypot Systems:

1) Honeypot plays a significant role in preventing the attacks and malicious activities.
2) It improves the attack detection time, response time.
3) It extracts the intrusion behaviour profiles, system behaviour and methods used to launch attacks.
4) It intercepts the behaviour patterns of adversary.
5) It records all the activities of Intruder.
6) They can be physically deployed or can be virtually set up.
7) Honeypots are expected to have zero false alarms.

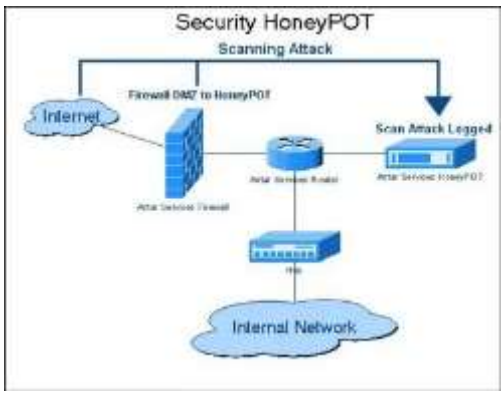

Figure.1 Honeypot Systems

Honeypots collect data which is of great value. It gathers precise data which is easy to understand. This facilitates easy analysis of data.

Honeypot is a system or computer that is deliberately "sacrificed" to be the target of attacks from hackers. The computer serves every attack done by hackers in the penetration of the server. This method is intended for the administrator of the server to be attacked to know the penetration tricks that hackers do and can anticipate in protecting the real server. Any action was taken by an intruder trying to connect to the honeypot, then the honeypot will detect and record it. A Honeypot is a source of information systems that are usually designed to detect, trap, in an attempt penetration into the system. Generally, the honeypot consists of computers, data, and network segments that look Honeypot also have a monitoring feature to monitor attacker activity when Enter into the honeypot system. Known activities include ports being attacked, commands typed by attackers, and alterations by attackers on a fake server honeypot. This can be exploited by the Network Administrator as input to patch the actual system, configuring the original network segment for early prevention.

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: Honeypots can capture attacks and give information about the attack type and if needed, thanks to the logs, it is possible to see additional information about the attack. New attacks can be seen and new security solutions can be created by looking at them. More examinations can be obtained by looking at the type of the malicious behaviors. It helps to understand more attacks that may happen. Honeypots are not bulky in terms of capturing data. They are only dealing with the incoming malicious traffic. Therefore, the information that has been caught is not as much as the whole traffic. Focusing only on the malicious traffic makes the investigation far easier. Therefore, this makes honeypots very useful. For the only malicious traffic, there is no need for huge data storage. There is no need for new technology to maintain. Any computer can be used as a honeypot system. Thus, it does not cost additional budget to create such a system.

Results: We studied all level of interaction honeypots and configured them. As first level of interaction honeypot, we deployed Honeyd. We explained the logic behind it and installed it correctly. Our findings about Honeyd are; Honeyd is the most popular low interaction honeypot but its problem is its age. The project is opensource but part of it is outdated and nobody seems to upgrade it. On the other hand hacker tools are evolving, so identifying this honeypot is not hard. Honeyd is using an old version on Nmap fingerprint to create fake virtual operating systems so by using a newer version of Nmap, the fake operating systems will not be recognized and Nmap will detect that there is a problem. Another limitation of Honeyd is the scripts bound to the different ports. With a basic scan it is possible to find which ports are open but as soon as the attacker tries to actually connect on a port, he will realize the service is fake. For example the script used for a Web server, by connecting it using telnet, thew server should send back replies but nothing is happening. Another problem is one cannot understand if there is an incoming attack to the system or not. Because there is no such alarm system that can make you understand that there is an attack. Information gathering is not very smart either. As a result the hacker can understand quickly that there is something wrong with the target and will abort his attack. Even unprofessional intruders can compromise the honeypot without spending too much time on it. Because it is very popular and easy to use well known techniques such as Nmap. There is no additional approach needed for it. Our second step was to configure medium level interaction honeypot Nepenthes. We explained how it works and how we studied on it in implementation part. However, we found some problems with Nepenthes too. First of all, Nepenthes is for capturing malware over internet. It is mostly used for this aim. Thus, it must be implemented very rapidly since threats for users over internet are increasing dramatically day by day. Nepenthes could not keep up with new threats. As new threats are arriving and Nepenthes is not up to date, it will not be able to capture malware. Another problem comes from the shellcode. Shellcode manager should consider about shellcode and understand it. As new threats cannot be captured, new exploits cannot be captured either. Furthermore, as we are investigating the problems and security flaws in our experiment, there is an important security flaw in Nepenthes structure. Nepenthes do not have transport layer security. Transport layer security is a protocol that gives security for communications throughout the internet. We think it is a real problem for honeypot deployment. Some malware exist on port 445 that are being involved with each other which are “LSASS, PNP, DCOM, ASN1, ms06-070, ms08-067”. When this kind of interference happens, we are not sure about the replies either. It creates a big mess between modules. (Schloesser M., (2009)). Figure 8.1 is showing the attacks observed according to Maheswari V. & Sankaranarayanan Dr.P.E., (2007).

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
8. Engineering , pp. 28-36, 2016.
9. 8. Thesis on "Honeypots in Network Security" by Deniz Akkaya-Fabien Thalgott, School of Computer Science, Physics and Mathematics, Linnaeus University, 29th June 2010.
10. Gérard Wagener. "Self-Adaptive Honeypots Coercing and Assessing Attacker Behaviour" Computer Science [cs]. Institut National Polytechnique de Lorraine - INPL, 2011. English.
11. 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.
12. 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,
13. 2011.

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.
14. L. Spitzner, Honeypots: Catching the insider threat, In: Computer Security Applications Conference 2003, Proceedings. 19th Annual. IEEE, 2003. p. 170-179, 2003
15. Dissertation on "Deception Techniques Using Honeypots" by Amit D. Lakhani, Information Security Group Royal Holloway, University of London, UK.
16. 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.