GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 10, Issue 5, May. (2022)

HONEYPOTS IN NETWORK SECURITY

Salimova Husniya Rustamovna
Master's degree, specialty "Information Security", Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

ABSTRACT

Security issues become one of the important aspects of a network, especially a network security on the server. These problems underlie the need to build a system that can detect threats from parties who do not have access rights (hackers) that are by building a security system honeypot. A Honeypot is a diversion of intruders' attention, in order for intruders to think that it has managed to break down and retrieve data from a network, when in fact the data is not important and the location is isolated. A way to trap or deny unauthorized use of effort in an information system. One type of honeypot is honeyd. Honeyd is a low interaction honeypot that has a smaller risk compared to high interaction types because the interaction with the honeypot does not directly involve the real system. The purpose of the implementation of honeypot and firewall, firewall is used on Mikrotik. Can be used as an administrative tool to view reports of Honeyd generated activity and administrators can also view reports that are stored in the logs in order to assist in determining network security policies.

Keywords: Honeypot, hacking, 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.

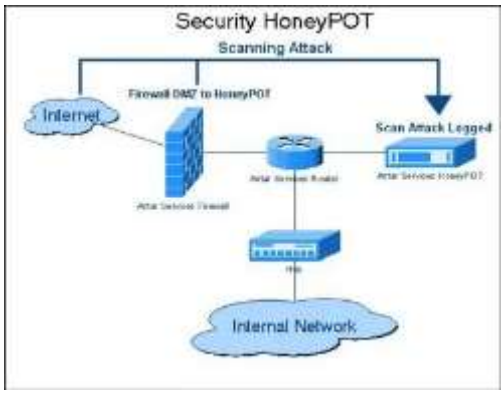

Figure.1 Honeypot Systems

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. A distributed system is proposed which remedy the existing deficiency in the centralised control system to improve network security and presents the experimental results which successfully improves the performance of the safety defence systems.

Honeypot technology has been widely used to overcome the limitations of firewall technology, many intrusion detection systems, intrusion prevention systems, which detected several attacks but couldnot detect new attacks. This paper discusses the honeypot technology according to the existed shortage in the honeypot system and proposes a distributed system which remedy the existing deficiency in the centralised control system to improve network security and presents the experimental results which successfully improves the performance of the safety defence systems.

MATERIALS

Honeypots do not face the problem of resource exhaustion unlike other security mechanisms. This is so because they capture data directed to them only. Thereby, less money needs to be spent on hardware for installing Honeypots. They are much cheaper as they do not require current technologies, RAM with huge capacity or disk drives.

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. 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

At the time of this est the author get the conclusion that the honeypot and firewall can cooperate in restraining the incident that occurred so the attacker can't enter easily because the attacker into the trap honeypot that has been made, so the server can work safely, and honeypot is successful in Detects suspicious activity and captures the attacker's IP and is stored in a separate folder on the server trap honeypot.

Like all technologies, honeypots have their drawbacks, the greatest one being their limited field of view. Honeypots capture only activity that's directed against them and will miss attacks against other systems.

For that reason, security experts don't recommend that these systems replace existing security technologies. Instead, they see honeypots as a complementary technology to network- and host-based intrusion protection.

The advantages that honeypots bring to intrusion-protection solutions are hard to ignore, especially now as production honeypots are beginning to be deployed. In time, as deployments proliferate, honeypots could become an essential ingredient in an enterprise-level security operation.

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.