A Review on Securing a Private Network using Honeypot

Shikha Malakar[1] Chetan Awasthi[2]

[1,2]School of Computer Science & Information Technology, DAVV Devi Ahilya Vishwavidyalaya
Takshashila Campus, Khandwa Road, Indore, Madhya Pradesh 452001, India

Abstract— Technology is being advanced day by day, more and more people are using internet all over the world. It is becoming a part of everyone's life. However, how many people are concerned about security? As technology is growing rapidly, newer attacks are appearing. The problem of security becomes even more critical in academic environment. The main aim of this research is to identify how Honeypot can be used in an academic environment to make it secure. Honeypot is a well-designed tool that is used to identify hackers. By using Honeypot, it is possible to monitor the activities started and running on the system by hacker. In other words, Honeypot is a trap machine which looks like a real machine and can be used to find out threats of a system. It is great way to improve security by getting the information from a victim system using forensic tool.

Key words: Firewall, Honeypot, IDS, IPS, Security, Vulnerability

I. Introduction

Computer and network have become very important part of our daily life. Now a day's use of internet is increased, therefore the requirement of its security is also increasing. There are many tools that are being used for making the network secure like Intrusion Detection System (IDS) Intrusion Prevention System (IPS), Firewall, and Antivirus etc. Honeypot is used to identify unknown vulnerabilities and threats that cannot be identified by firewall and other means of security. The major difference between Honeypot and others is that other tools of security can only be used with known attacks and threats, whereas Honeypot can also be used to identify the unknown one. One can get early warnings of new vulnerabilities by installing and monitoring computer systems on a network that we expect to be broken into. Every attempt to contact these systems via the network is suspect. Such a system is called Honeypot. The idea behind it is more focused on the defensive side and to develop the powerful technologies and tools like Firewall and Intrusion Detection System (IDS) to defend the network from intruders. It is concerned in the types of attacks; the various tools used for attacking, the new kinds of virus and other security threats so that systems can be defended more securely. The idea behind the Honeypot is to create a virtual system, put the system visible to the attackers so that they can be compromised and probe. The system will keep track of all the activities and later the logged information is analyzed to make sure the system and to identify new types of threats. If a Honeypot is compromised, then the information collected is used to identify the vulnerability that was used to compromise it.

Lance Spitzner defines Honeypot technology as –"A Honeypot is security resource whose value lies in being probed, attacked, or compromised."[6].

II. Background

The strength of good security is to have security in depth. Honeypot complements other types of security, without replacing them. It is used as part of a comprehensive security policy and adds an additional layer of protection to detect security breaches that may not be identified by other means.

A. Firewall:

A firewall prevents access by blocking connections according to a rule base. A hacker attacking a network protected by a firewall will be prevented from even identifying the services that are running. Honeypot however, allows connection but sends a back a response in case of attack [1].

B. Anti-Virus Software:

Anti-Virus software uses a signature database to identify known viruses, Trojans and worms. It examines hard disk or the contents of email attachments to identify malware. Honeypot detects the actions performed by malware and are reported immediately. Another advantage of Honeypot is that it is effective at detecting new viruses that have not yet been added to the anti-virus signature database by anti-virus software vendors [1].

C. Network Based Intrusion Detection Systems (NIDS):

NIDS perform the task of monitoring the traffic on the network looking for known attack patterns within the data being transferred. Because NIDS also rely on the signature database techniques as anti-virus software they suffer the same problems with new attack patterns. They can also wrongly identify legitimate traffic as suspicious. Often the false positives can overwhelm the reporting of genuine attacks.

Honeypot also contains a signature database to identify know attacks, but it is not dependent on this to detect an attack [1].

D. Honeypot:

The main value of Honeypot lies on being attacked so that the administrator can study their attackers and kinds of attacks. Therefore it can be said that Honeypot is a tool that study the world of internet security, to identify the various threats and vulnerabilities. From the introduction, we know that the main objective of the Honeypot is to collect information. Honeypot can be used for two reasons for a production or research purposes. The production Honeypot measures the existing network vulnerability with outside threat and a research, studies the attackers so that they can be better equipped for the future attacks.

The main aim of Honeypot is: to know who our enemy is. If follows the saying again best defense to our security is to have best offense. The more one is aware of the current security issues, the more one get secured. The other aspect of the Honeypot is we don't have to go around hackers' computer to look for the information; the hacker himself comes to us [3].

III. Review

Several papers were published in the area of Honeypot and Information Security. The various papers were studied. Many types of Honeypots have been developed depending upon the area and use.

Several papers were published in the area of Honeypot and network security. The various papers were studied.

A paper on “Honeyd: A Virtual Honeypot Daemon” [10] was studied. This paper provided a brief overview of the design and implementation of Honeyd, a daemon that simulates the TCP/IP stack of operating systems to create virtual Honeypots. Then the paper discussed the design and implementation of Honeyd. It discussed intended goals and show how they were implemented. It defines how virtual Honeypot is configured using templates. New templates are created with the create command. The set and add commands change the configuration of a template. It gave a brief overview of Honeyd’s design and implementation. Evaluation of paper showed that Honeyd is effective in creating virtual routing topologies and successfully fools fingerprinting tools.

A paper on “HoneyAnalyzer - Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot”[11] was studied. This paper stated the intrusion detection signature; the purpose of attack signatures is to describe the characteristic element of attack. In Intrusion Detection Signature there is a common standard for defining signature. This paper then proposed a method for defining signature for Honeypot which includes data capture, data analysis and signature extraction to extract a good quality signature.

A paper on “Honeypot Security” [8] was studied. This paper defined what a Honeypot is. It stated that, a Honeypot works by fooling attackers into believing it is a legitimate system; they attack the system without knowing that they are being observed covertly. When an attacker attempts to compromise a Honeypot, attack-related information, such as the IP address of the attacker, will be collected. This activity done by the attacker provides valuable information and analysis on attacking techniques, allowing system administrators to “trace back” to the source of attack if required. This paper also classified the Honeypot into Low interaction and High interaction Honeypot. A High interaction Honeypot gives attacker real system to interact with whereas a Low interaction does not. This paper also stated strategies to deploy a Honeypot to maximize the strength and to minimize the risk involved. Finally it gives the example of Honeypot systems.

A paper on “An Improved Hybrid Intrusion Detection System in Cloud Computing” [2] was studied. This paper had 3 phases; in phase one only KFsensor is used to provide security to the network. In phase 2 analyses using Flowmatrix is done. At last in phase 3 both KFsensor and Flowmatrix is used to build a Hybrid system that can overcome the drawbacks of KFsensor and Flowmatrix when used alone.

A paper on “HoneyDroid - Creating a Smartphone Honeypot” was studied. This paper suggests the use of Honeypot in android mobile devices. It suggests a design based on micro kernel to identify and threat.

S.N	Method	Year	Pros	Cons
1.	Honeyd: Introduction, design and implementation.	2003	Honeyd is effective for creating virtual routing topologies.	No inbuilt log analyzer is present.
2.	Data Capture, Analysis for Signature Extraction.	2005	Good for extracting good quality signature from the data obtained by the logs of Honeypot.	Requires deep analysis to build narrow signature.
3.	Definition of Honeypot its classification and deployment.	2008	Brief introduction of Honeypot and its examples was given.	Only theoretical overview of Honeypot is given.
4.	Creating a Honeypot for android mobile phones.	2011	Micro kernel provides strong isolation guarantees for its applications.	Does not behave exactly the same way original Android system does, as some virtualization overhead has to be taken into account.
5.	Deployment of KFsensor and Flowmatrix to build a Hybrid intrusion detection system.	2012	Drawbacks of KFsensor and Flowmatrix can be overcome, when implemented together.	No means are introduce to automatically analyze the logs generated.

Table 1: Literature Review Table

IV. Conclusion

Network Security has span diverse disciplines from business to research. Currently there are quite number or research has been conducted based on honeypot security. Honeypot are new technology which is to be used to give the network security, from threats for organizations .This paper gives a review of the work and studies done in the field of network security and Honeypot.

REFERENCES

[1] Focus, K. (2003). KFSensor overview.

[2] Gautam, A. K., Sharma, V., & Prakash, S. (2012). An Improved Hybrid Intrusion Detection System in Cloud Computing. International Journal of Computer Applications, 53(6), 1-13.

[3] Gurung, S. KFSensor Vs Honeyd.

[4] https://en.wikipedia.org/wiki/Honeypot_%28computing%29

[5] Karthik Sadasivam, Banuprasad Samudrala, T. Andrew Yang University of Houston – Clear Lake 2700 Bay Area Blvd., Houston, TX 77058 (281) 283-3835, yang@cl.uh.edu

[6] Lance Spitzner “Honeypots: Tracking Hackers”, (Addison Wesley 2002)

[7] Lee, K., Caverlee, J., & Webb, S. (2010, April). The social Honeypot project: protecting online communities from spammers. In Proceedings of the 19th international conference on World wide web (pp. 1139-1140). ACM

[8] Miliefsky, G. (2008). U.S. Patent No. 7,346,922. Washington, DC: U.S. Patent and Trademark Office.

[9] Mulliner, C., Liebergeld, S., & Lange, M. (2011, May). Poster: Honeydroid-creating a smartphone honeypot. In IEEE Symposium on Security and Privacy.

[10] Provos, N. (2003, February). Honeyd-a virtual Honeypot daemon. In 10th DFN-CERT Workshop, Hamburg, Germany (Vol. 2, p. 4) Pouget, F., & Dacier, M. (2004, May). Honeypot-based forensics. In AusCERT Asia Pacific Information Technology Security Conference.

[11] Thakar, U., Varma, S., & Ramani, A. K. (2005, September). HoneyAnalyzer–analysis and extraction of intrusion detection patterns & signatures using Honeypot. In Proceedings of the Second International Conference on Innovations in Information Technology.