# Implementation of Honeypot in Academic Environment

**Shikha Malakar[1] Mr. Chetan Awasthi[2]**
[2]Lecturer
[1,2]Department of Computer Science & Information Technology
[1,2]DAVV Devi Ahilya Vishwavidyalaya Takshashila Campus, Khandwa Road, Indore, Madhya Pradesh 452001, India

*Abstract*— Honeypot Technology has been widely used to overcome the limitations of existing technologies like firewall, Intrusion detection system (IDS), Intrusion prevention system (IPS), antivirus etc. These systems can detect several known attacks but are not able to find out unknown attacks. This paper discus the Honeypot technology according to its implementation in an academic environment and present the experimental result, which successfully improves the performance of the security system used in an academic environment.

***Key words:*** DOS, Firewall, Honeypot, IDS, IPS, Vulnerability

## I. INTRODUCTION

Today with the help of internet it has become very easy to communicate with the whole world. To detect threats and security breaches it is important to be up-to-date with the hacker's innovation. Various security defense systems were used but they could not detect attacks inside an organization network [13]. Also they could not recognize the new attacks.To overcome these problems Honeypot technology was introduced.

"Honeypots can be defined as the attractive defence resource placed inside a network that attracts the attackers towards it, with the actual intention to capture new attacks and learn the tools and techniques used by them"[11].

## 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. PROPOSED APPROACH

The approach for practical implementation will be to implement a windows based Honeypot system in the college network. I will be using KFsensor for this. This would be done in two phases. In first phase KFsensor will be implemented in a wired network. Then in second phase it will be implemented in a wireless network. After both the implementations the result obtained from both the phases will be analyzed for a comparative study.

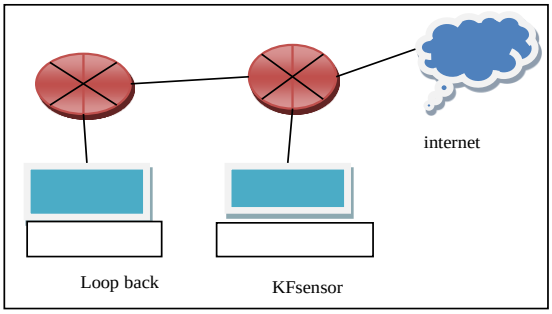


Fig. 1: Proposed approach work architecture

 

## IV. IMPLEMENTATION AND RESULTS

### *A. Phase 1*

KFsensor was implemented in Local Area network (LAN) of college .KFsensor was implemented in a system with windows 8.1 and was used as Honeypot. A simple ping operation was performed followed by a continuous ping operation using –t command. Following was the result found after completion of both operations.

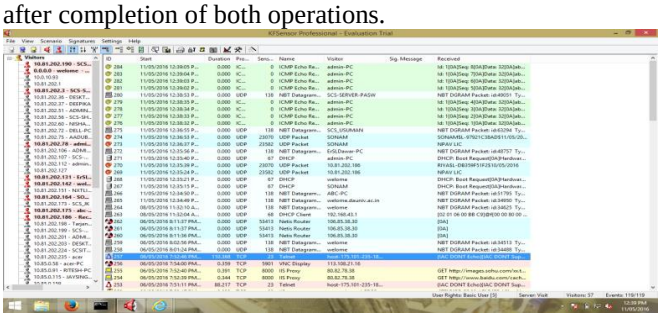

Fig. 2: A Simple Ping Operation in Wired Network

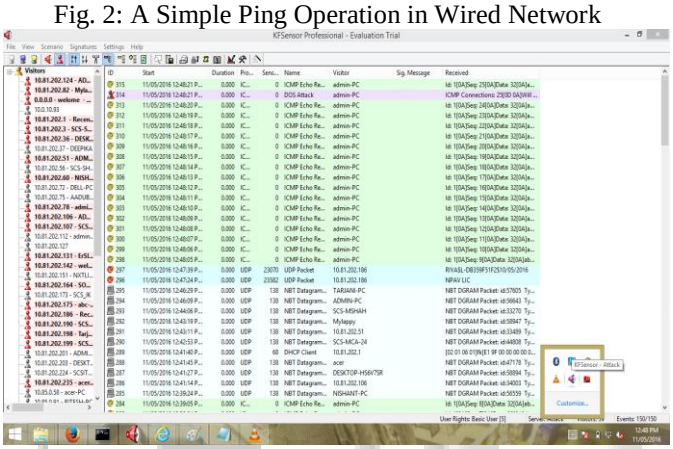

Fig. 3: A Continuous Ping Operation in Wired Network

| Type of Service | Name of service | Protocol | Severity | Icon |
|---|---|---|---|---|
| Connection | NBT datagram service | UDP | Low | |
| Connection | DHCP | UDP | Low | |
| Native Connection | DHCP Client | UDP | Low | |
| DOS Attack | DOS Attack | ICMP | Low | |
| ICMP Ping | ICMP Echo Request | ICMP | Medium | |
| Closed Port | UDP Packet | UDP | High | |

Table 1: A Table of KF Sensor Log Study for Wired Network

### *B. Phase 2*

KFsensor was implemented in wireless network (Wi-Fi) of college .KFsensor was implemented in a system with windows 8.1 and was used as Honeypot. A simple ping operation between two laptops was performed .Following was the result found after completion of the operation.

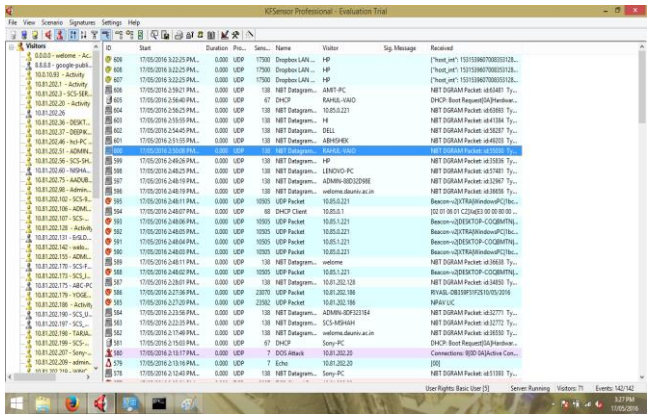

Fig. 4: A Simple Ping Operation in Wi-Fi Network

| Type of Service | Name of service | Protocol | Severity | Icon |
|---|---|---|---|---|
| Connection | NBT datagram service | UDP | Low | |
| Connection | DHCP | UDP | Low | |
| Native Connection | DHCP Client | UDP | Low | |
| DOS Attack | DOS Attack | ICMP | Low | |
| ICMP Ping | ICMP Echo Request | ICMP | Medium | |
| Native Connection | NBT SMB | TCP | Medium | |
| Connection | Echo | TCP | Medium | |
| Connection | Dropbox LAN Sync | UDP | Medium | |
| Closed Port | UDP Packet | UDP | High | |
| Closed Port | TCP Closed Port | TCP | High | |
| Closed Port | TCP Syn Scan | TCP | High | |

Table 2: A Table of KF Sensor Log Study for Wireless Network

## V. SUMMARY AND CONCLUSION

The objective of this research is to remedy the limitations of the existing security tools by implementing KFsensor in a wired and wireless network. The proposed approach shows better durability, efficiency for better network security. With the wide use of honeypot technology attackers always try to follow the track which is not a honeypot. Because now they know, they can be easily detected. Issues must be focussed in the future about how to secure our systems with the hacker's new innovations from causing harm and damage to the network security.

## 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) 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
[7] Miliefsky, G. (2008). U.S. Patent No. 7,346,922. Washington, DC: U.S. Patent and Trademark Office.
[8] Mulliner, C., Liebergeld, S., & Lange, M. (2011, May). Poster: Honeydroid-creating a smartphone honeypot. In IEEE Symposium on Security and Privacy.
[9] 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.
[10] Ritu Tiwari, Abhishek Jain (2012 ,october). Design and Analysis of Distributed Honeypot System. In Proceedings of the International Journal of Computer Applications (0975 – 8887) Volume 55– No.13, October 2012.
**[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.
[12] Y. Yang, H. Yang, and J. Mi, Design of Distributed Honeypot System Based on Intrusion Tracking, IEEE. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference. Xi'an, China.

 