A Review paper on the survey on honeypot technology

Heena

CSE,PTU GZS CAMPUS

BATHINDA,INDIA

1610heena@gmail.com

Abstract:Honeypots are physical or virtual machines successfully used as intrusion detection tools to detect worm-infected hosts.In the area of information security,honeypots refers to a closely monitored computing resource that we want to be probed,attacked or compromised.In this paper we present an overview of intrusion detection systems and a brief discussion on honeypots.The trend towards grouping honeypots into honeynets and Honeyd, HoneyBOT, and Specter honeypotswill also be discussed.

I. INTRODUCTION

The information security is an ever increasing concern of organizations and individuals in this age.The information security techniques have started to take different forms from the traditional techniques used in the past as attacks have become more sophisticated.Honeypot is an information system resource whose value lies in the unauthorized use of the resources. Located either in or outside the firewall, the honeypot is used to learn about an intruder's techniques as well as determine vulnerabilities in the real system. Traditionally, IDS's have been used by network administrators to actively monitor network traffic for unauthorized activity. However, in today's world of increasingly encrypted connections, which intrusion detection systems are unable to monitor, honeypots have become an increasingly attractive alternative to locate sources of malicious traffic.

Honeypots, first created in 1998, function by recording all connections and connection attempts. A honeypot system should be placed on an unused IP address, such that no legitimate connection attempt would ever be directed to the honeypot. Two main types of honeypots are available today: high-interaction and low-interaction. Low-interaction honeypots are simple and provide partial implementations of common protocols, with the goal of recording only the source of malicious traffic. High-interaction honeypots are more complex and often are regular servers with advanced monitoring software and have the goal of helping researchers understand hacker's internal thought processes.

Honeypots are still an advancing field of computer science, with recent developments creating world-wide networks of honeypots, commonly referred to as honeynets and distributed honeypots.

II. TYPES OF HONEYPOTS

- Low Interaction Honeypots:Low Interaction Honeypots allow only limited interaction for an attacker or malware. All services offered by a Low Interaction Honeypots are emulated. Thus Low Interaction Honeypots are not themselves vulnerable and will not become infected by the exploit attempted against the emulated vulnerability.
- High Interaction Honeypots:High Interaction Honeypots make use of the actual vulnerable service or software. High-interaction honeypots are usually complex solutions as they involve real operating systems and applications. In High Interaction Honeypots nothing is emulated everything is real. High Interaction Honeypots provide a far more detailed picture of how an attack or intrusion progresses or how a particular malware execute in real-time. Since there is no emulated service, High Interaction Honeypots helps in identifying unknown vulnerabilities. But High Interaction Honeypots are more prone to infections and High Interaction Honeypots increases the risk because attackers can use these real honeypot operating systems to attack and compromise production systems.

III. ADVANTAGES AND DISADVANTAGES OF HONEYPOTS

A. Advantages:

- Honeypots collect very little data, and what they do collect is normally of high value. This cuts the noise level down, make it much easier to collect and archive data. One of the greatest problems in security is wading through gigabytes of data to find the data you need. Honeypots can give you the exactly the information you need in a quick and easy to understand format. For example, the Honeynet Project, a group researching honeypots, collects on average only 1-5MB of data per day. This information is normally of high value also, as not only can you show network activity, but also what the attacker does once he or she gets on the system.

- Simplicity: The very simplicity of design, implementation and use makes a honeypot a desirable method to enhance security conditions in any organization.
- Resources: Many security tools can be overwhelmed by bandwidth or activity. Network Intrusion Detection Devices may not be able to keep up with network activity, dropping packets, and potentially attacks. Centralized log servers may not be able to collect all the system events, potentially dropping some events. Honeypots do not have this problem, they only capture that which comes to them.
- Honeypots are a great training environment for security professionals.

1) *Disadvantages:*

- Single Data Point: Honeypots all share one huge drawback; they are worthless if no one attacks them. Yes, they can accomplish wonderful things, but if the attacker does not send any packets to the honeypot, the honeypot will be blissfully unaware of any unauthorized activity.
- Risk: Honeypots can introduce risk to your environment. Different honeypots have different levels of risk. Some introduce very little risk, while others give the attacker entire platforms from which to launch new attacks. Risk is variable, depending on how one builds and deploys the honeypot.

- There is also the temptation to retaliate. One should be careful and stay within legal means. Returning tit for tat only gets one in trouble. The goal is to increase ones own security, not go to war with the script kiddies.
- Honeypots won't fulfill their promise unless one has the time to administer them correctly. Companies concerned about security threats are "better off using an intrusion-detection system" if they don't have a dedicated team of highly trained administrators. But many administrators, torn by budget constraints and the need to find quick-fix solutions to get critical systems back online, often are in no position to probe cracker attacks, says Frank Prince, an electronic-security analyst with Forrester Research in Cambridge, Mass.

What's more, in dollar terms the most damaging attacks come from inside companies, not from crackers. While honeypots can help compile information on people breaking into the system, they do little to combat sabotage from within.

Thus though honeypots can add value, the time and resources involved may best focused on greater priorities. It is because of these disadvantages that honeypots do not replace any security mechanisms. They can only add value by working with existing security mechanisms.

IV. RECENT TRENDS AND ADVANCES OF HONEYPOTS

In reviewing the literature, it became apparent that the research can be broken down into five major areas:

- new types of honeypots to cope with emergent new security threats,
- utilizing honeypot output data to improve the accuracy in threat detections
- configuring honeypots to reduce the cost of maintaining honeypots as well as to improve the accuracy in threat detections
- counteracting honeypot detections by attackers
- legal and ethical issues in using honeypots.

V. RECENT HONEYPOT PRODUCTS

- HoneyBOT is a windows based low interaction honeypot solution.HoneyBOT works by opening a large range of listening sockets on your computer from which a selection of these sockets are designed to mimic vulnerable services. When an attacker connects to these services they are fooled into thinking they are attacking a real server. The honeypot safely captures all communications with the attacker and logs these results for future analysis. Should an attacker attempt an exploit or upload a rootkit or trojan to the server the honeypot environment can safely store these files on your computer for malware collection and analysis purposes.
- Honeyd is a small daemon that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating systems. Honeyd enables a single host to

claim multiple addresses - I have tested up to 65536 - on a LAN for network simulation. Honeyd improves cyber security by providing mechanisms for threat detection and assessment. It also deters adversaries by hiding real systems in the middle of virtual systems. Honeyd is created for Unix Operating Systems and Honeyd is open source software released under GNU General Public License.

- KFSensor is a Commercial Windows based honeypot Intrusion Detection System (IDS).It acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and trojans.By acting as a decoy server it can divert attacks from critical systems and provide a higher level of information than can be achieved by using firewalls and NIDS alone.

VI. CONCLUSION

The purpose of this paper was to define the what honeypots are and their value to the security community. We identified two different types of honeypots, low-interaction and high-interaction honeypots. Interaction defines how much activity a honeypot allows an attacker. The value of these solutions is both for production or research purposes. Honeypots can be used for production purposes by preventing, detecting, or responding to attacks. Honeypots can also be used for research, gathering information on threats so we can better understand and defend against them.

REFERENCES

[1] Babak Khosravifa, JamalBentaha, “An experience improving intrusion detection systems false alarm ratio by using Honeypot,” 22nd International Conference on Advanced Information Networking and Applications, 2008.

[2] Mohan Krishnamurthy, Eric S. Seagren, “Network Analysis, Troubleshooting, and Packet Sniffing,” How to Cheat at Securing Linux, pp. 203-247, 2008.

[3] Sándor Molnár, Balázs Sonkoly, Tuan Anh Trinh, “A comprehensive TCP fairness analysis in high speed networks,” Computer Communications, vol. 32, Issues 13-14, pp. 1460-1484, August 2009.

[4] Angela Orebaugh, Becky Pinkard, “Nmap OS Fingerprinting,” Nmap in the Enterprise, pp. 161-183, 2008.

[5] Chi-Ho Tsang, Sam Kwong, Hanli Wang, “Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection,” Pattern Recognition, vol. 40, Issue 9, pp. 2373-2391, September 2007.

[6] Cheng Xiang, Png Chin Yong, Lim Swee Meng, “Design of multiple-level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees,” Pattern Recognition Letters, vol. 29, Issue 7, pp. 918-924, 2008.

[7] Chia-Mei Chen, Ya-Lin Chen, Hsiao-Chung Lin, “An efficient network intrusion detection,” Computer Communications, vol. 33, Issue 4, pp. 477-484, March 2010.

[8] Benjamin Morin, Ludovic Mé, Hervé Debar, Mireille Ducassé, “A logic-based model to support alert correlation in intrusion detection,” Information Fusion, vol. 10, Issue 4, pp. 285-299, October 2009.

[9] Xiaojun Tong, Zhu Wang, Haining Yu, “A research using hybrid RBF/Elman neural networks for intrusion detection system secure model,” Computer Physics Communications, vol. 180, Issue 10, pp. 1795-1801, October 2009.

[10] W. Acosta and S. Chandra, “Trace driven analysis of the long term evolution of gnutella peer-to-peer traffic,” in PAM, 2007, pp. 42–51.

[11] S. Sen and J. Wang, “Analyzing peer-to-peer traffic across large networks,” IEEE/ACM Trans. Netw., vol. 12, no. 2, pp. 219–232, 2004.

[12] Y. Kulbak and D. Bickson, “The emule protocol specification,” School of Computer Science and Engineering The Hebrew University of Jerusalem, Tech. Rep., January 2005.

[13] J.-L. Guillaume, M. Latapy, and S. Le-Blond, “Statistical analysis of a p2p query graph based on degrees and their timeevolution,” in IWDC, 2004, pp. 126–137.

[14] S. Le-Blond, J.-L. Guillaume, and M. Latapy, “Clustering in p2p exchanges and consequences on performances,” in IPTPS, 2005, pp. 193–204.

[15] F. Aidouni, M. Latapy, and C. Magnien, “Ten weeks in the life of an edonkey server,” in Proceedings of HotP2P’09, 2009.

[16] E. Adar and B. A. Huberman, “Free riding on gnutella,” First Monday, vol. 5, 2000.